



Victorian
Law Reform
Commission



WARNING
PREMISES UNDER
CONSTANT
SURVEILLANCE



SURVEILLANCE IN PUBLIC PLACES

Final Report 18

GPO Box 4637
Melbourne Victoria 3001 Australia
DX 144, Melbourne

Level 3, 333 Queen Street
Melbourne Victoria 3000 Australia

Telephone: + 61 3 8619 8619
Freecall: 1300 666 555 (within Victoria)
Facsimile: + 61 3 8619 8600
Email: law.reform@lawreform.vic.gov.au
Web: www.lawreform.vic.gov.au

Contents

Preface	5	Major users of public place surveillance	32
Terms of reference	6	Victoria Police	32
Glossary	7	Corrections Victoria	34
Executive summary	11	Local councils	34
Recommendations	15	Public housing	35
Chapter 1: Introduction	19	Universities and TAFEs	35
Introduction	20	Transport	35
Background	20	Major public events: concerts and sports	38
Important definitions	21	Crown Casino	39
What is surveillance?	21	The hospitality industry	40
What is a public place?	22	Shopping centres and retailers	40
Coverage of this report	22	The media	41
Federal areas of concern	22	Marketing companies	41
State law enforcement	23	Private investigators	41
Practices covered by information privacy laws	23	Public and private insurers	42
Other law reform activity	24	The private security industry	42
Australian Law Reform Commission	24	Aged care	42
NSW Law Reform Commission	24	Personal uses	42
New Zealand Law Commission	25	Conclusion	43
UK House of Lords Select Committee	25	Chapter 3: Current Law	45
Hong Kong Law Reform Commission	26	Introduction	46
Law Reform Commission of Ireland	26	Surveillance devices legislation	46
Our process	26	Information privacy legislation	47
Consultation Paper	26	Information privacy laws and public place surveillance	48
Final Report	26	Enforcement of information privacy laws	49
Outline of this report	27	Regulation of specific aspects of public place surveillance	50
Chapter 2: Use of Surveillance in Public Places	29	Common law protections	51
Introduction	30	The Victorian Charter of Human Rights and Responsibilities	51
Surveillance technology	31	Limits on the right to privacy under the Charter	52
Closed-circuit television (CCTV)	31	Non-binding guidelines, standards and policies	52
GPS and satellite technology	31	Regulation in other jurisdictions	53
Tracking mobile phones	31	Other Australian jurisdictions	53
Radio frequency identification (RFID)	31	Other countries	54
Automatic number plate recognition (ANPR)	31	Conclusion	54
Body imaging devices and scanners	32	Table 1: Legislation and binding codes relating to public place surveillance in Victoria	55
Biometric technologies	32	Table 2: Major non-binding instruments relating to public place surveillance in Victoria	57
Google Earth and Google Streetview	32		

Chapter 4: A Balanced Approach to Regulation	59	Significant surveillance users: ensuring responsible practice	93
Introduction	60	Significant users of public place surveillance	93
The impact of public place surveillance	60	Reviewing advice prepared by significant users of public place surveillance	96
Benefits	60	Examining the practices of significant users of public place surveillance	96
Investigation of criminal activity and fraud	61	Advising of a significant user's failure to comply	96
Asset protection and deterrence of crime	61	Reporting to parliament	97
Safety	62	Investigations and proceedings in relation to SDA breaches	98
Operational needs	63	The most appropriate body to regulate public place surveillance	99
Managing the movement and conduct of people	63	Relationship with other surveillance regulators	100
News gathering and the dissemination of information	63	Review of Victoria Police surveillance practices	101
Artistic purposes, entertainment and other personal uses	63	Regulatory features not recommended at this stage	103
Risks	64	Registration or licensing of some surveillance users	103
Threat to privacy	64	A complaint-handling power for the regulator	104
Social exclusion	64	General own-motion investigatory powers	104
Loss of anonymity	66	Procurement standards as a tool to encourage compliance	105
The chilling effect	66	Conclusion	105
Criminal conduct and offensive uses	68	Chapter 6: Modernising the Surveillance Devices Act	107
Publication on the internet	68	Introduction	108
Surveillance may not work	69	Background	108
Converging devices	71	Definitions	108
A balanced approach to regulation	71	Private activity	108
The Victorian Charter of Human Rights and Responsibilities	71	Implied consent	110
Regulatory theory	75	Prohibition of surveillance devices in toilets	112
An overview of our recommendations and our approach	80	Regulated tracking devices	112
Conclusion	80	Automatic number plate recognition	114
Chapter 5: Promoting Responsible Use of Surveillance in Public Places	83	Management and care of patients	115
Introduction	84	Removing the participant monitoring exception	117
Principles to govern the use of surveillance in public places	84	Allowing some instances of participant monitoring	117
Six public place surveillance principles	85	A civil penalty regime	121
An independent regulator of public place surveillance	89	A new offence for improper use of a surveillance device	122
Regulatory functions	90	Other jurisdictions	124
Encouraging responsible practice	90	Conclusion	125
Research and monitoring	90		
Educating, providing advice and promoting understanding of laws and best practice	91		
Developing and publishing best practice guidelines	91		

Contributors

VICTORIAN LAW REFORM COMMISSION

Chairperson

Professor Neil Rees*

Commissioner

Associate Professor Pamela O'Connor

Part-time Commissioners

Paris Aristotle AM*

Magistrate Mandy Chambers

Hugh de Kretser*

Her Honour Judge Felicity Hampel

Professor Sam Ricketson*

Justice Iain Ross AO*†

Reference Team

Emily Minter (Team leader)

Miriam Cullen

Sally Finlay

Lara Rabiee

Chief Executive Officer

Merrin Mason

Operations Manager

Kathy Karlevski

Team Leaders

Emma Cashen Lindy Smith

Emily Minter Myra White

Policy and Research Officers

Becky Batagol Ian Parsons

Freia Carlton Lara Rabiee

Zane Gaylard Martin Wimpole

Kirsten McKillop Hilda Wrixon

Research Assistants

Sarah Dillon Alexandra Krummel

Melleta Elton Tess McCarthy

Amanda Kite Jessica Saunders

Communications Officer

Carlie Jennings

Project Officer

Simone Marrocco

Assistant Operations Manager

Vicki Christou

Research and Executive Assistant

Mia Hollick

Librarian

Julie Bransden

Administrative Officers

Failelei Siatua Samuel Tucker

* Commissioners involved in this reference.

† Retired March 2010.

Contents

Chapter 7: Statutory Causes of Action	127
Introduction	128
Civil action for serious invasion of privacy	128
The law in Australia	128
The law in the UK	130
The law in New Zealand	134
The law in the United States	137
The law in Canada	140
Other law reform commission recommendations	141
Australian Law Reform Commission	141
NSW Law Reform Commission	143
Should Victoria enact a cause of action for invasion of privacy?	145
The commission's recommendation: two statutory causes of action	147
Misuse of private information	149
Intrusion upon seclusion	150
Statutory causes of action	151
Elements	151
Defences	153
Exemptions?	159
Remedies	160
Costs	163
Jurisdiction	163
Availability of the cause of action to corporations and deceased persons	164
Limitation of action	166
Conclusion	167
Appendices	169
Appendix A: Submissions	170
Appendix B: Consultative Committee, Community Forums, Consultations and Site Visits	172
Appendix C: Preliminary Roundtable Consultations	174
Bibliography	176

Preface

This report completes a two-stage inquiry into the widespread use of privacy invasive technologies. The first stage of our inquiry dealt with workplace privacy, while this report deals with the growing use of surveillance in public places.

Public place surveillance is so extensive that it now affects the lives of nearly all Victorians. It is highly likely that our image will be captured by camera, and recorded, whenever we are walking down city streets, travelling on public transport, driving on freeways, visiting shopping centres or attending a major sporting event. People should know about these activities and appreciate that it is becoming increasingly difficult to remain anonymous in public places. The notion of blending in with the crowd is fast disappearing.

The Attorney-General asked the commission to consider the interests of users of surveillance in protecting their 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 report reflects the diversity of opinion regarding the use of surveillance in public places. We must seek to reap the many benefits of modern surveillance equipment while also ensuring that it is not used oppressively and unnecessarily in public places.

Existing laws were not designed with the use of high technology surveillance devices in mind. This report contains 33 recommendations for reform. Our proposed regulatory model encourages the responsible use of surveillance in public places. It balances this with the protection of individual rights, especially the right to privacy.

Similar reviews of public place surveillance have taken place or are occurring elsewhere. In February 2010 the New Zealand Law Commission recommended new laws to deal with the misuse of visual surveillance, interception and tracking devices. In the UK, the interim CCTV Regulator will make recommendations by the end of 2010 for regulation of the use of CCTV in public places.

Devising regulatory responses to significant technological change is often challenging. That has proven to be the case in this instance. I express my thanks to the members of the division of the commission who worked with me on this reference—Justice Iain Ross AO, Professor Sam Ricketson, Paris Aristotle AM and Hugh de Kretser—and who gave generously of their time and expertise. In particular, I wish to acknowledge the contribution of Professor

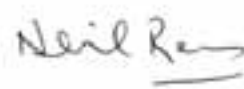
Sam Ricketson who chaired this division prior to my appointment to the VLRC. Justice Ross resigned from the VLRC upon being appointed President of the Victorian Civil and Administrative Tribunal (VCAT) in March 2010. The recommendation in Chapter 7 concerning VCAT was devised well before this date.

All members of the commission team who worked on this project have produced high quality work. Team Leader Emily Minter played a central role in the preparation of this report. Her commitment, understanding of the issues and organisational skills were of vital importance. Policy and Research officers Miriam Cullen and Lara Rabiee made major contributions to the entire report, while Sally Finlay and Padma Raman participated in overall planning and worked on particular chapters. Melleta Elton, Mia Hollick, Simone Marrocco, Claire Roberts and Suzanne Zhou provided research assistance. The report was edited by Clare Chandler and produced by Carlie Jennings.

Many others made important earlier contributions to this reference. Former Team Leader Emma Cashen coordinated the later consultation stage of the reference and the publication of our Consultation Paper. Priya SaratChandran made a contribution to research and consultation, and to our understanding of the many complex issues which should be individually recognised. Michelle Burrell and Bronwyn Jennings gave early research and writing assistance. Vicki Christou and Failelei Siatua provided administrative support.

In 2009 we established a consultative committee to provide us with advice. I thank the members of that committee—Louise Connor, Andy Frances, Leigh Gassner, Moira Paterson, Michael Pearce SC, Bill Penrose, Jen Rose, Helen Versey and Deane Wilson—for their very helpful responses to our draft recommendations.

One of the members of that committee, Associate Professor Moira Paterson, has acted as a consultant and adviser throughout this reference. We benefited greatly from her expertise and wise counsel.



Professor Neil Rees

Chairperson

May 2010

Terms of Reference

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

- a. whether legislative or other reforms should be made to ensure that workers' privacy, including that of employees, independent contractors, outworkers and volunteers, is appropriately protected in Victoria. In the course of this inquiry, the commission should consider activities such as
 - surveillance and monitoring of workers' communications;
 - surveillance of workers by current and emerging technologies, including the use of video and audio devices on the employers' premises or in other places;
 - physical and psychological testing of workers, including drug and alcohol testing, medical testing and honesty testing;
 - searching of workers and their possessions;
 - 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).

Glossary

Automatic number plate recognition (ANPR)	Technology that recognises symbols in images of a number plate and stores or uses those symbols to identify the vehicle.
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 in which 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 that utilises serious measures only when milder sanctions (such as education) have failed.
e-tag	A device attached to a vehicle that 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.

Glossary

Global positioning system (GPS)	A navigation system that relies on information received from a network of satellites to provide the latitude and longitude of an object or location.
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 enables 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	<i>See Visual surveillance.</i>
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.
Olfactory surveillance	Purposeful monitoring of a person or object by smell, including by the use of a device or animal.
Panopticon	A type of prison building designed by Jeremy Bentham to facilitate 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 enables 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 that is read using energy from an RFID reader.
Text message/SMS	The exchange of brief written messages between mobile phones and other portable devices over cellular networks. Messages can now also include image, video and sound content (known as MMS messages).
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 that, 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, object or place.
Tort	A breach of a duty, imposed by law, that protects the bodily integrity, property, reputation or other interests of a person.

Glossary

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 regions 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 that enables the 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

INTRODUCTION

This is the Victorian Law Reform Commission's Final Report for 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*. In this report we consider surveillance in public places.

Surveillance devices have become increasingly affordable, available and sophisticated. Their use has proliferated. Current laws were not designed to deal with the many ways in which these devices are used in Victorian public places. In this report the commission makes a series of recommendations that seek to modernise the existing regulatory regime. The recommendations strive to encourage responsible surveillance practices and ensure that users of surveillance devices do not infringe the rights of the Victorian public.

BACKGROUND

Government agencies, private organisations and individuals use public place surveillance extensively. Victorians can expect to be observed, recorded and tracked while engaging in daily activities in streets, shopping centres and major public venues.

The capabilities of surveillance devices are also increasing rapidly. Surveillance devices are able to locate individuals in a crowd, determine identity, track movements, record conversations, and compile and share this information almost instantaneously. As technologies become more sophisticated, so, too, do the applications for which they are used. For example, devices may be used at airports to see through passengers' clothing, or identify individuals from within hundreds of cars on a freeway.

Many groups within our community rely heavily on surveillance technology in their everyday activities, including police, transport operators, retailers, private investigators, sports venues and journalists. Surveillance serves a number of important purposes, including the promotion of public safety, the prevention and investigation of crime, and newsgathering. In addition, many widely owned personal products, such as mobile phones, have surveillance capabilities.

Negative consequences that may flow from the increased use of surveillance in public places include a loss of privacy and anonymity. One concern is that this may cause Victorians 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. Those people with the means to do so may retreat to private places whenever possible in order to avoid unwanted observation.

In devising recommendations for reform, the commission has taken into account the many benefits that arise from the use of public place surveillance, as well as the risks posed by its misuse.

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 they are federal responsibilities. We recommend that the surveillance activities of state law enforcement bodies be considered separately because of the need to consider police investigation and information gathering activities as a whole.

CONSULTATIVE PROCESS

In March 2009 the commission published a Consultation Paper that was informed by extensive preliminary consultations. We presented a number of options for reform and received detailed feedback in over 40 submissions from government agencies, private organisations and community advocates.

We also hosted five forums with groups who experience public place surveillance, including young people, people experiencing homelessness, and culturally and linguistically diverse communities. We established a consultative committee of individuals with different experiences of public place surveillance whom we consulted on a number of occasions. In addition, we met members of the community, and visited major Victorian surveillance users at their premises in order to gain a thorough understanding of their use of surveillance technologies.

These submissions, consultations and meetings provided us with a thorough understanding of the scope, nature and impact of public place surveillance in Victoria (outlined in Chapter 2), and the benefits and risks that flow from its use (outlined in Chapter 4).

CURRENT LAW

There is little regulation of the use of surveillance devices in public places. Existing laws are unclear, they have not kept pace with technological change, and they do not appear to be actively enforced. There is a widespread uncertainty among surveillance users and the community about which surveillance activities are permitted in public places. The three major bodies of relevant law—the *Surveillance Devices Act 1999* (Vic) (SDA), the *Privacy Act 1988* (Cth) and the *Information Privacy Act 2000* (Vic)—were not specifically designed to regulate public place surveillance.

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.

No clear public policy emerges from these separate laws concerning the circumstances in which public place surveillance is acceptable and those when it is not. We consider the current regulatory framework in Chapter 3.

A BALANCED APPROACH TO REGULATION

Numerous benefits arise from the use of surveillance devices, including crime prevention and investigation, crowd control and the dissemination of information. However, there are also risks associated with its use, including the increased loss of people's anonymity and personal space in public. The commission proposes a regulatory regime that is based on a set of overarching principles that seek to balance the many competing interests at play and are flexible enough to allow for rapid changes in technology. This approach is primarily educative and focuses on achieving best practice use of surveillance technology, while also ensuring that the privacy rights of individuals are adequately protected.

Two sources that provide a framework for achieving a balanced approach to regulation, and which have informed our recommendations, are the *Charter of Human Rights and Responsibilities Act 2006* (Vic) (the Victorian Charter) and theories of responsible regulation. We discuss the applicability of these sources to the development of our approach in Chapter 4.

ENCOURAGING RESPONSIBLE USE

Users of surveillance frequently stated that they were unsure of what surveillance they could lawfully undertake and would welcome further guidance in this area. Our recommendations aim to provide greater certainty about appropriate uses of surveillance in any particular circumstance.

The commission proposes a set of overarching legislative principles to guide all users about responsible use of public place surveillance. The principles, set out in Chapter 5, are based on those proposed in our Consultation Paper. The Victorian Charter framework for balancing competing interests, and the principles contained in privacy legislation, informed our approach. In refining these principles we drew upon the opinions expressed in submissions and consultations, and the views of our Consultative Committee.

The six public place surveillance principles devised by the commission are as follows.

1. People are entitled to a reasonable expectation of privacy when in public places.
2. Users of surveillance devices in public places should act responsibly and consider the reasonable expectations of privacy of individuals.
3. Users of surveillance devices in public places should take reasonable steps to inform people of the use of those devices.
4. Public place surveillance should be for a legitimate purpose related to the activities of the organisation conducting it.
5. Public place surveillance should be proportional to its legitimate purpose.
6. Reasonable steps should be taken to protect information gathered through public place surveillance from misuse or inappropriate disclosure.

These principles are discussed in Chapter 5.

The commission recommends the creation of an independent regulator. The primary roles of the regulator would be to promote the responsible use of surveillance in public places by providing practical guidance to surveillance users, to provide the public with information about their rights, and to keep the government and the people of Victoria fully informed of rapidly changing technology. In Chapter 5 we consider the range of functions and powers necessary for the regulator to fulfil these tasks, bearing in mind that the least restrictive regulatory methods are desirable.

Although appropriate guidance about the responsible use of surveillance in public places is a cornerstone of our recommendations, guidance alone cannot protect people from some practices that seriously affect their privacy. Chapters 6 and 7 deal with additional regulatory measures for particularly offensive uses of surveillance.

MODERNISING THE SURVEILLANCE DEVICES ACT

To reflect changes to the way surveillance is used in Victoria, and to ensure that the law keeps pace with advances in technology, the commission recommends a number of changes to clarify, modernise and strengthen the SDA. The SDA primarily prohibits the use of covert surveillance devices in private places, while also allowing law enforcement use of surveillance with a warrant. The commission's proposed recommendations include amending some important definitions to reflect contemporary uses of surveillance devices, and expressly prohibiting surveillance in toilets and change rooms. Another recommendation is the introduction of a prohibition on participant monitoring (where a person records an activity or conversation to which they are a party without the consent of other parties), which is currently allowed under the Act.

Executive Summary

The commission also recommends the introduction of a new offence to prohibit highly offensive uses of surveillance devices, regardless of where the surveillance occurs. This offence is designed to send a clear message to the community that various forms of behaviour are unacceptable, including, for example, filming violence for entertainment (happy slapping). Using surveillance to intimidate or prevent people from doing something they are otherwise lawfully entitled to do, like attending an abortion clinic or drug treatment centre, would also be covered by the offence.

In addition, we recommend that a civil penalty regime also apply to existing criminal offences in the SDA. This would provide for greater flexibility in enforcement by allowing a surveillance regulator to act on the less serious matters that come to his or her attention without referring the matter to Victoria Police for criminal prosecution.

STATUTORY CAUSES OF ACTION

The commission believes that individual Victorians should be able to take civil action in response to serious invasions of privacy by the use of surveillance in a public place.

At present, no Australian jurisdiction has enacted a statutory cause of action for invasion of privacy, and no appellate court has acknowledged the existence of a common law tort of invasion of privacy.

It is open to both the High Court and the Victorian Court of Appeal to recognise a common law tort of invasion of privacy in the absence of any legislative action. However, developments in other common law countries, most notably the UK and New Zealand, suggest it will take a long time before a reasonably clear body of law emerges.

Legislation would provide greater clarity and certainty within a more acceptable timeframe. The *Charter of Human Rights and Responsibilities Act 2006* (Vic) (the Charter) is a useful catalyst for legislative action because 'privacy' is one of the human rights that parliament specifically seeks to protect and promote under the Charter.

The commission recommends the introduction of two statutory causes of action for serious invasions of privacy: the first dealing with misuse of private information, the second with intrusion upon seclusion.

Although our focus is an appropriate legal response to the misuse of surveillance in public places, these new causes of action would not necessarily be limited to conduct that occurred in a public place or that involved the use of a surveillance device.

Recommendations

GENERAL

1. The Victorian parliament should enact new laws that promote the responsible use of surveillance devices in public places.

PRINCIPLES

2. The legislation should include the following guiding principles.
 1. People are entitled to a reasonable expectation of privacy when in public places
 2. Users of surveillance devices in public places should act responsibly and consider the reasonable expectations of privacy of individuals
 3. Users of surveillance devices in public places should take reasonable steps to inform people of the use of those devices
 4. Public place surveillance should be for a legitimate purpose related to the activities of the organisation conducting it
 5. Public place surveillance should be proportional to its legitimate purpose
 6. Reasonable steps should be taken to protect information gathered through public place surveillance from misuse or inappropriate disclosure.

REGULATOR OF PUBLIC PLACE SURVEILLANCE

3. A regulator should be responsible for the oversight of public place surveillance in Victoria.
4. The regulator should have the following functions in relation to public place surveillance:
 - a. research and monitoring, including use, technologies and current laws
 - b. educating, providing advice and promoting understanding of laws and best practice
 - c. developing and publishing best practice guidelines
 - d. reviewing advice prepared by public authorities and significant private users of public place surveillance
 - e. examining the practices of public authorities and significant private users in relation to their public place surveillance practices
 - f. advising a public authority or significant private organisation of any failure to comply with laws and best practice guidelines
 - g. investigating and taking civil proceedings in relation to potential breaches of the SDA
 - h. reporting to the Minister on an annual basis on any matters in relation to any of its functions, including any failure by public authorities and significant organisations to comply with advice under paragraph (f).
5. Public authorities and significant private users should be required to provide advice to the regulator annually on their compliance with public place surveillance guidelines in relation to designated surveillance devices.
6. The Victorian government should define 'significant private user' for the purposes of the regulatory regime.

Recommendations

7. In addition to any other powers conferred on the regulator by legislation, the regulator should have the power to do all things necessary or convenient for, or in connection with, the performance of the functions of the regulator.
8. In addition to his or her annual reporting function, the regulator should also have the power to report formally to the relevant Minister about any matters relating to his or her functions. The Minister should be required to table all reports provided by the regulator in parliament.
9. The functions of the regulator should be exercised by the Victorian Privacy Commissioner.
10. The Commissioner for Law Enforcement and Data Security should conduct a review of, and create guidelines for, Victoria Police's use of surveillance and surveillance-captured data.

MODERNISING THE SURVEILLANCE DEVICES ACT

11. The words '*an activity carried on outside a building*' should be removed from the definition of 'private activity' in section 3 of the SDA so that it reads:

private activity means an activity carried on in circumstances that may reasonably be taken to indicate that the parties to it desire it to be observed only by themselves, but does not include an activity carried on in any circumstances in which the parties to it ought reasonably to expect that it may be observed by someone else.
12. The SDA should be amended so that courts are directed to consider whether a public place surveillance user has given adequate notice of their surveillance activities when considering whether a person has given 'implied consent' to any of the conduct that falls within sections 6–9 and 11–12 of the SDA.
13. The SDA should be amended to expressly prohibit the use of an optical surveillance device or listening device to observe, listen to, record or monitor any activity in toilets, shower areas and change rooms which form a part of any public place. This prohibition should include a law enforcement exemption similar to that in section 9B(2) of the SDA.
14. The definition of 'tracking device' in section 3 the SDA should be amended so that it includes all electronic devices capable of being used to determine the geographical location of a person or object.
15. The Governor in Council should be permitted to make regulations that allow specific law enforcement activities to be exempted from the general prohibition in section 8 of the SDA against using a tracking device without consent.
16. The proposed new regulator should advise Parliament regularly about the use of ANPR technology in Victoria, including whether the current regulatory controls are adequate.
17. The automatic substitute consent regime in Part 4A of the *Guardianship and Administration Act 1986 (Vic)* should be extended so that the 'person responsible' may consent to the installation of a tracking device for a person over the age of 18 years who is incapable of giving consent to the installation of that device.
18. Sections 6 and 7 of the SDA should be amended to prohibit participant monitoring using a listening or optical surveillance device subject to the following additional exceptions:

- a. the use of a listening or optical surveillance device by a law enforcement officer to record a private conversation or private activity to which he or she is a party if:
 - i) the law enforcement officer is acting in the course of his or her duty; and
 - ii) the law enforcement officer reasonably believes at least one party to the conversation or activity of having committed or being in the course of committing an offence
 - b. the use of a listening device or optical surveillance device by a party to a private conversation or private activity if:
 - i) a principal party to the conversation or activity consents to the listening device being so used; and
 - ii) recording of the conversation or activity is reasonably necessary for the protection of the lawful interests of that principal party.
19. Sections 6–9 and 11–12 of the SDA should be amended to include civil penalties as an alternative to criminal penalties. The regulator should be permitted to commence proceedings for the imposition of a civil penalty.
20. A new offence should be included in the SDA that makes it unlawful to use a surveillance device in such a way as to:
- a. intimidate, demean or harass a person of ordinary sensibilities; or to
 - b. prevent or hinder a person of ordinary sensibilities from performing an act they are lawfully entitled to do.
21. A civil and alternative criminal penalty should apply for breach of the offence. The regulator should be permitted to commence proceedings for the imposition of a civil penalty.

CREATING STATUTORY CAUSES OF ACTION

22. There should be two statutory causes of action dealing with serious invasion of privacy caused by misuse of surveillance in a public place.
23. The first cause of action should deal with serious invasion of privacy by misuse of private information.
24. The second cause of action should deal with serious invasion of privacy by intrusion upon seclusion.
25. The elements of the cause of action for serious invasion of privacy caused by misuse of private information should be:
- a. D misused, by publication or otherwise, information about P in respect of which he/she had a reasonable expectation of privacy; and
 - b. a reasonable person would consider D’s misuse of that information highly offensive.
26. The elements of the cause of action for serious invasion of privacy caused by intrusion upon seclusion should be:
- a. D intruded upon the seclusion of P when he/she had a reasonable expectation of privacy; and
 - b. a reasonable person would consider D’s intrusion upon P’s seclusion highly offensive.

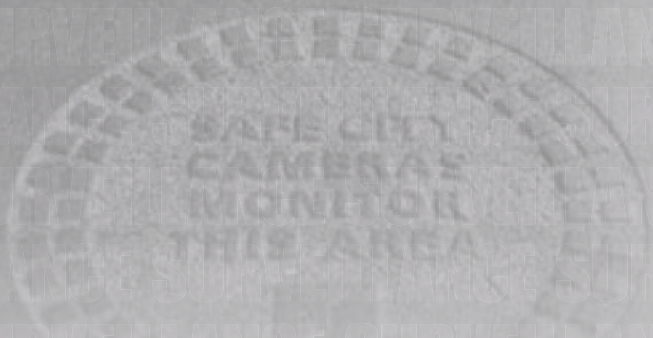
Recommendations

27. The defences to the cause of action for serious invasion of privacy caused by misuse of private information should be:
 - a. P consented to the use of the information
 - b. D's conduct was incidental to the exercise of a lawful right of defence of person or property, and was a reasonable and proportionate response to the threatened harm
 - c. D's conduct was authorised or required by law
 - d. D is a police or public officer who was engaged in his/her duty and the D's conduct was neither disproportionate to the matter being investigated nor committed in the course of a trespass
 - e. if D's conduct involved publication, the publication was privileged or fair comment
 - f. D's conduct was in the public interest, where public interest is a limited concept and not any matter the public may be interested in.
28. The defences to the cause of action for serious invasion of privacy caused by intrusion upon seclusion should be:
 - a. P consented to the conduct
 - b. D's conduct was incidental to the exercise of a lawful right of defence of person or property, and was a reasonable and proportionate response to the threatened harm
 - c. D's conduct was authorised or required by law
 - d. D is a police or public officer who was engaged in his/her duty and the D's conduct was neither disproportionate to the matter being investigated nor committed in the course of a trespass
 - e. D's conduct was in the public interest, where public interest is a limited concept and not any matter the public may be interested in.
29. The remedies for both causes of action should be:
 - a. compensatory damages
 - b. injunctions
 - c. declarations.
30. Costs should be dealt with in accordance with section 109 of the VCAT Act.
31. Jurisdiction to hear and determine the causes of action for serious invasion of privacy by misuse of private information and by intrusion upon seclusion should be vested exclusively in the Victorian Civil and Administrative Tribunal.
32. These causes of action should be restricted to natural persons. Corporations and the estates of deceased persons should not have the capacity to take proceedings for these causes of action.
33. Proceedings must be commenced within three years of the date upon which the cause of action arose.

Chapter 1 Introduction

CONTENTS

- 20 Introduction
- 20 Background
- 21 Important definitions
- 22 Coverage of this report
- 24 Other law reform activity
- 26 Our process
- 27 Outline of this report



Introduction

INTRODUCTION

- 1.1 This is the Victorian Law Reform Commission's Final Report into surveillance in public places. The Victorian Attorney-General asked the Victorian Law Reform Commission (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. The first phase of the reference concluded in 2005 with the publication of the commission's *Workplace Privacy: Final Report*.¹
- 1.2 The terms of reference for the second phase asked the commission to consider whether there is appropriate control of surveillance in public places.² In January 2009 we produced *Surveillance in Public Places: Consultation Paper* (Consultation Paper) in which we presented a number of options for reforming the law to better regulate surveillance of public places.³ We have since received submissions and engaged in consultations on the options we presented. In this report we present our final recommendations.
- 1.3 The terms of reference also asked us to consider whether the commission's proposed model to regulate surveillance of workers could be applied in relation to the regulation of surveillance in public places. There are a number of similarities between the two sets of recommendations (including our proposal for the introduction of overarching principles to guide legislative changes, and a 'light-touch' regulatory approach). This is explained in more detail in Chapters 4 and 5.

BACKGROUND

- 1.4 Surveillance devices have become increasingly available, affordable and sophisticated, and their use in public places has proliferated. For example, many local councils in Victoria now operate closed-circuit television (CCTV) systems. Police, transport authorities, sporting and entertainment venues and retail outlets also use CCTV. In addition, the capacity to use information gathered by CCTV systems is expanding. Many modern CCTV systems are now networked, and images can be stored, searched, analysed, reproduced and made available on the internet.
- 1.5 A variety of location and tracking devices is also being used in Victorian public places to determine the whereabouts and movement of individuals. They include the use of global positioning system (GPS) technology in phones and cars, and automatic number plate recognition (ANPR) technology on freeways. Google's Street View application allows internet users to view and zoom in on photographs of Australian streetscapes, and, potentially, individuals.⁴ The federal government has also recently announced its intention to introduce body scanners at international airports, which will effectively enable security personnel to see through passengers' clothing.⁵
- 1.6 Many common products now have surveillance capabilities. One obvious example is mobile phones,⁶ many of which have the capacity to record images and sounds and to transmit them to multiple destinations, almost instantaneously and at low cost.
- 1.7 Numerous benefits arise from the use of surveillance devices, including crime prevention, investigations, crowd control and the dissemination of information. However, there are also risks, including the increased loss of individuals' anonymity and personal space in public, particularly as devices can monitor movement and capture information in ways not previously possible.

- 1.8 Although research has shown community support for the use of some types of surveillance in public places,⁷ this support is not absolute. There are concerns about the potential loss of privacy in public places, the potential misuse of collected information, the potential discriminatory effect of surveillance and the lack of evidence supporting the effectiveness of surveillance in achieving its stated purposes.⁸ 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.⁹
- 1.9 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 do not always know whether they are acting lawfully when engaging in surveillance practices. Because surveillance technology is developing so rapidly, and laws are subsequently becoming outdated, it is time to consider how best to encourage the responsible use of surveillance devices while also protecting the rights and interests of individuals who may be harmed by their misuse.

IMPORTANT DEFINITIONS

WHAT IS SURVEILLANCE?

- 1.10 The term 'surveillance' stems from the French word *surveiller*, meaning 'to watch over'.¹⁰ The *Macquarie Dictionary* defines surveillance as the 'watch kept over a person, etc., especially over a suspect, a prisoner, or the like'.¹¹ Other definitions emphasise the motivation for the conduct in question. For example, David Lyon, one of the foremost academics in this area, defines surveillance as 'the focused, systematic and routine attention to personal details for the purposes of influence, management, protection or directions'.¹²
- 1.11 In our Consultation Paper we said that surveillance may be a once off or systematic activity, it may be conducted using a device or by personal observation, and it usually involves deliberate rather than incidental conduct. Accordingly, the commission suggested that surveillance should be defined as 'the deliberate or purposive observation or monitoring of a person or object'.¹³
- 1.12 There was general support in consultations and submissions for this definition, although some consultees raised specific concerns. In particular, there was concern that the definition refers only to the monitoring of people and objects. It was suggested that some users of surveillance could potentially avoid regulation by arguing that their use of surveillance protects or monitors a place or area.¹⁴
- 1.13 We have amended our definition of surveillance in response to this concern. In this report we use the term surveillance to mean the deliberate or purposive observation or monitoring of a person, object or place.
- 1.14 The expansion of the definition to include 'place' means that cameras installed to observe a general area, such as an outdoor mall or park, would constitute surveillance.¹⁵ We consider this definition broad enough to cover the many surveillance practices undertaken in Victoria without risk of over-inclusion.¹⁶

- 1 Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005).
- 2 The terms of reference are reproduced on page 6.
- 3 Victorian Law Reform Commission, *Surveillance in Public Places*, Consultation Paper No 7 (2009).
- 4 Andrew Colley, 'Privacy Advocates Say Google's Gone Too Far', *The Australian* (Sydney), 5 August 2008, 3.
- 5 Anthony Albanese MP, Minister for Transport, 'Strengthening Aviation Security' (press release, 9 February 2010).
- 6 Mobile phone subscriber penetration rates in Australia were estimated at being between 110% and 115% of the population in August 2009: Paul Budde, *Australia: Mobile Communications Subscriber Statistics*, (2004) Paul Budde Communication Pty Ltd <www.budde.com.au/Research/Australia-Mobile-Communications-Subscriber-Statistics.html> at 5 March 2010.
- 7 See Helene Wells et al, *Crime and CCTV in Australia: Understanding the Relationship* (2006) i-iii, 50; Wallis Consulting Group, *Community Attitudes to Privacy 2007: Prepared for Office of the Privacy Commissioner Reference No WG3322* (2007) 3, 74-5; 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.
- 8 Submissions 5, 7, 12, 14, 18, 19, 27, 30, 32, 34, 40, 42, 43. For a discussion on the effectiveness of CCTV, see Wells, above n 7, 47-50; see also Wallis Consulting Group, above n 7, 74-5.
- 9 See eg 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; Roundtable 16.
- 10 *Oxford English Dictionary* (10th ed rev, 2002) 1443.
- 11 Colin Yallop et al (eds), *Macquarie Dictionary* (4th ed, 2005) 1418.
- 12 David Lyon, *Surveillance Studies: An Overview* (2007) 14.
- 13 Victorian Law Reform Commission, above n 3, 11.
- 14 Consultation 9.
- 15 Although monitoring of a place will necessarily include the monitoring of activities conducted, or changes that occur to objects within that place, we have included 'place' in our definition to make it clear that we mean to cover this type of surveillance.
- 16 This is also consistent with the definition adopted by the NSW Law Reform Commission. See NSW Law Reform Commission, *Surveillance: Final Report*, Report No 108 (2005).

Introduction

WHAT IS A PUBLIC PLACE?

- 1.15 In our Consultation Paper, we noted that it was difficult to draw a clear line between a ‘public place’ and a ‘private place’.¹⁷ We suggested that any attempt to do so should focus on the nature and degree of accessibility to a place by members of the public, rather than whether a place is privately or publicly owned.
- 1.16 Drawing on the definition contained in the *Racial Discrimination Act 1975* (Cth), we suggested that ‘public place’ should be defined as ‘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’.¹⁸
- 1.17 Thus ‘public places’ include public areas such as parks and streets, as well as government or privately owned places when they are open to the general public, such as shopping centres, libraries, sporting arenas and local swimming pools. This definition received general support in consultations and submissions.

COVERAGE OF THIS REPORT

- 1.18 Despite our broad definitions of ‘public place’ and ‘surveillance’ we have not examined all forms of public place surveillance in Victoria. We have not, for example, considered surveillance that occurs in workplaces because we addressed this in the first phase of our privacy reference. 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.¹⁹
- 1.19 Other practical considerations and constitutional constraints have also limited our field of inquiry. These are outlined below.

FEDERAL AREAS OF CONCERN

- 1.20 Section 109 of the Commonwealth Constitution says that where state and federal laws are inconsistent, the federal law should prevail to the extent of the inconsistency. Thus, in developing our options for reform of Victorian law, we must consider its interaction with relevant areas of Commonwealth concern.

Telecommunication and data surveillance

- 1.21 The *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA) regulates the interception of telecommunications and access to communications stored in 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.
- 1.22 The High Court has decided that the TIA exclusively regulates interception of telephone communications.²⁰ It is also highly likely that the TIA exclusively regulates interceptions of other communications that take place across telecommunications networks, such as 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.²¹ These limitations mean that the Victorian regulation of listening devices, in particular, is important in protecting communications across public networks.

- 1.23 The existence of the TIA also limits the ability of the Victorian government to regulate cyberspace surveillance. Most practices involving the use of computer software to spy on the activities of others via the internet²² involve telecommunications interceptions. Further, the borderless nature of cyberspace makes it impractical to regulate at a state level. For these reasons, we have not considered cyberspace-related surveillance in this inquiry. We do note, however, the importance of appropriate regulation in this area.²³
- 1.24 Other data surveillance that is incidental to the activities regulated by the TIA but does not actually fall within the scope of the Act is 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

- 1.25 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 and other national security organisations, specific powers to engage in surveillance activities for security purposes.²⁴ Recently, these powers were greatly expanded by a series of laws that form part of a package of anti-terrorism measures.²⁵ Australian Security Intelligence Organisation (ASIO) officers, for example, are permitted to use tracking devices in accordance with a ministerial warrant 'despite any law of a State or Territory'.²⁶

STATE LAW ENFORCEMENT

- 1.26 The commission believes that regulation of police use of surveillance is best achieved through an entirely separate regime from the one we propose for general users of surveillance. For this reason, and others, we have not undertaken a comprehensive review of the police use of surveillance in public places.
- 1.27 Surveillance is one of many means of investigation and crime detection available to police. Examining the police use of surveillance in isolation from other investigative tools would not be a fruitful exercise. In addition, some police use of surveillance is subject to warrant-based processes under the *Surveillance Devices Act 1999* (Vic) (SDA) and other state and Commonwealth laws. Police officers are subject to sanctions that do not apply to other surveillance users and, with judicial authorisation, they may engage in activities that are otherwise prohibited.
- 1.28 A number of specialist bodies monitor the operations of Victoria Police, including access to its data. The commission recommends that such a body undertake a review of police use of surveillance technology and surveillance-captured data. This proposal is dealt with in Chapter 5.

PRACTICES COVERED BY INFORMATION PRIVACY LAWS

- 1.29 The primary focus of this report and our recommendations is surveillance practices—that is, the practices associated with observing and recording a person's behaviour. Although we have considered the use of information gathered by the use of surveillance (including the purposes for which it is used, and procedures relating to retention, security and provision third parties), we have not focused specifically on the 'personal information' that may be collected by surveillance practices.

- 17 These difficulties have been noted by commentators 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.
- 18 *Racial Discrimination Act 1975* (Cth) s 18C.
- 19 Standing Committee of Attorneys-General, *Unauthorised Photographs on the Internet and Ancillary Privacy Issues* Discussion Paper (2005).
- 20 See *Miller v Miller* (1978) 141 CLR 269, 276.
- 21 *Telecommunications (Interception and Access) Act 1979* (Cth) s 5.
- 22 Eg the use of viruses or worms such as Trojan or rootkit malware infections.
- 23 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) <www.austlii.edu.au/itlaw/articles/TaiwanSTLC.html> at 19 November 2008; Cyber Law Policy Centre at the University of NSW <www.bakercyberlawcentre.org/> at 3 December 2008.
- 24 Eg the *Surveillance Devices Act 2004* (Cth).
- 25 Eg changes under the *Anti-Terrorism Act (No. 2) 2005* (Cth).
- 26 *Australian Security Intelligence Organisation Act 1979* (Cth) s 26A.

Introduction

- 1.30 Commonwealth and state information privacy laws regulate the use of ‘personal information’.²⁷ These laws contain privacy principles concerning the collection, storage and use of personal information. While information privacy laws may regulate some uses of public place surveillance,²⁸ many of these activities are likely to be beyond the reach of privacy laws.
- 1.31 Information privacy laws apply to government agencies and large businesses only.²⁹ In order to be defined as ‘personal information’, information must be recorded,³⁰ and must be about an individual ‘whose identity is apparent, or can reasonably be ascertained’.³¹ The extent to which surveillance-captured information is covered by this description is discussed in Chapter 3. Most information captured by surveillance practices is unlikely to be ‘personal information’ for the purposes of information privacy laws because the identity of an individual cannot ‘reasonably be ascertained’ from that information.
- 1.32 However, because some ‘personal information’ is capable of being captured by surveillance practices, there is potential for overlap between information privacy laws and any regulation of surveillance. We have developed our recommendations with this issue in mind.

OTHER LAW REFORM ACTIVITY

- 1.33 The issues of surveillance and privacy have been the subject of recent reports by other Australian and international law reform bodies. The work of those bodies has informed the commission’s approach to the complex issues surrounding public place surveillance. We have referred to the findings of these law reform agencies throughout the report.

AUSTRALIAN LAW REFORM COMMISSION

- 1.34 In August 2008 the Australian Law Reform Commission (ALRC) reported on whether the *Privacy Act 1988* (Cth) and related laws continue to provide an effective framework for the protection of privacy in Australia.³² The report included 295 recommendations, which, if implemented, will result in a large-scale overhaul of privacy regulation in Australia.
- 1.35 In its report, the ALRC recommended the creation of a unified set of privacy principles that would apply to all federal government agencies and the private sector. The ALRC also recommended that these principles should apply to state and territory government agencies through an intergovernmental cooperative scheme. This model aimed to ensure that, subject to limited exceptions, the same privacy principles would apply across Australia.
- 1.36 The Australian Government released the first stage of its response to the ALRC proposals in October 2009.³³ It made an extensive commitment to redrafting the *Privacy Act 1998* (Cth) and giving new powers to the Privacy Commissioner. The ALRC proposals, and the government response to them, are discussed in more detail in Chapter 3 of this report.
- 1.37 The ALRC recommended a federal statutory cause of action for invasion of privacy that would be available to individuals whose privacy has been invaded by means of surveillance. This proposal assisted us when developing recommendations, set out in Chapter 7, about two new causes of action for misuse of surveillance.

NSW LAW REFORM COMMISSION

- 1.38 In 2005, the NSW Law Reform Commission (NSWLRC) published a report entitled *Surveillance: Final Report* which proposed a broad legislative approach to regulating covert and overt forms of surveillance in private and public places.³⁴

1.39 More recently, the NSWLRC released a report (*Invasion of Privacy*) that examined the adequacy of NSW personal information and health information legislation, with a view to providing an effective framework for the protection of individuals' privacy.³⁵ This report also recommended the development of a statutory cause of action for invasion of privacy.

NEW ZEALAND LAW COMMISSION

1.40 In March 2009 the New Zealand Law Commission (NZLC) released an issues paper on the adequacy of New Zealand's civil and criminal laws in dealing with invasions of privacy. They found a number of significant gaps in the law.³⁶

1.41 In February 2010 the NZLC published its final report, *Invasion of Privacy: Penalties and Remedies*, which recommended a comprehensive model to reform the gaps identified in the existing law regulating the use of surveillance in New Zealand. Central to these recommendations was the creation of a new Surveillance Devices Act that would establish both civil and criminal remedies in relation to the misuse of visual surveillance, interception and tracking devices.³⁷

UK HOUSE OF LORDS SELECT COMMITTEE

1.42 In January 2009 the House of Lords Select Committee on the Constitution released a report into surveillance.³⁸ Entitled *Surveillance: Citizens and the State*, the report made 44 recommendations on issues such as greater government monitoring of surveillance (particularly in the private sector), secure storage of personal data and investment in technology to help protect privacy.³⁹

1.43 The UK government issued a response to the report in May 2009 in which it addressed each of the recommendations. The government agreed to undertake consultation on a number of issues, but challenged the need for greater regulation in the private sector and observed that it found many of the government's current practices to be adequate.⁴⁰ The UK Home Office has also established an interim independent regulator for CCTV in the UK.

27 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.

28 See *WL v La Trobe University* [2005] VCAT 2592; *Smith v Victoria Police* [2005] VCAT 654; *Ng v Department of Education* [2005] VCAT 1054; *Re Pasla and Australian Postal Corporation* (1990) 20 ALD 407; *Kiernan v Commissioner of Police, NSW Police* [2007] NSWADT 207. See also 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.

29 Large businesses are defined as those with a turnover of over \$3 million. *Privacy Act 1988* (Cth) s 6(D).

30 *Privacy Act 1988* (Cth) s 16B; *Information Privacy Act 2000* (Vic) s 3.

31 *Privacy Act 1988* (Cth) s 6(1); *Information Privacy Act 2000* (Vic) s 3.

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

33 Australian Government, *Australian Government First Stage Response to the Australian Law Reform Commission Report 108: For Your Information: Australian Privacy Law and Practice* (2009).

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

35 NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009).

36 New Zealand Law Commission, *Invasion of Privacy: Penalties and Remedies Review of the Law of Privacy Stage 3*, Issues Paper 14 (2009) [5.30].

37 New Zealand Law Commission, *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy: Stage 3*, Report 113 (2010).

38 Select Committee on the Constitution, House of Lords, *Surveillance: Citizens and the State: Volume 1: Report 2nd Report of Session 2008–9* (2009).

39 Ibid.

40 See eg, UK Government, *Response to the House of Lords Selection Committee on the Constitution's Report Surveillance: Citizens and the State* (2009).

Introduction

HONG KONG LAW REFORM COMMISSION

- 1.44 The Hong Kong Law Reform Commission (HKLRC) has released a number of reports considering surveillance related issues. Of particular relevance to our inquiry is the report *Privacy: The Regulation of Covert Surveillance*.⁴¹ Legislation enacted in 2006 adopted the recommendations in the HKLRC's report by prohibiting covert surveillance without judicial authorisation.⁴²

LAW REFORM COMMISSION OF IRELAND

- 1.45 In 1998, the Law Reform Commission of Ireland released a report into surveillance.⁴³ A parliamentary working group subsequently released another report on privacy in 2006.⁴⁴ Some of the recommendations from the surveillance report informed the drafting of the *Criminal Justice (Surveillance) Act 2009* which provides for the use of covert surveillance by authorisation in relation to criminal investigations.⁴⁵

OUR PROCESS

CONSULTATION PAPER

- 1.46 The commission's first step was to hold 31 roundtable discussions with organisations including police, local councils, universities, transport operators, media, entertainment venues, retailers, courts, security organisations, as well as representatives of young people, the indigenous community, state government and other community representatives.
- 1.47 The purpose of these consultations was to provide the commission with a broad understanding of the way organisations and individuals use surveillance in public places and how their use affects people. The consultations also helped us to understand what 'surveillance' and 'public places' mean to members of the community and to gauge their understanding of existing relevant laws.
- 1.48 In March 2009 we published a Consultation Paper, which was informed by our consultations as well as extensive secondary research. The paper described current uses of public place surveillance in Victoria and examined likely future trends. The paper also explored the concept of privacy, provided an overview of the relevant law in Victoria and other jurisdictions, and considered the risks and benefits associated with public place surveillance. Finally, the Consultation Paper presented a number of options for reform, designed to stimulate public discussion. We called for submissions and posed 24 questions to guide responses. These responses informed the recommendations in this report.

FINAL REPORT

- 1.49 This Final Report is the product of a year-long period of consultation and research in which we sought feedback on the proposals made in our Consultation Paper, and information about the scope, nature, and impact of public place surveillance in Victoria.

Submissions and consultations

- 1.50 The commission received 44 written submissions in response to our Consultation Paper from a variety of organisations and individuals, including community representatives, human rights advocacy groups, legal organisations and users of surveillance technology.⁴⁶

- 1.51 In addition, we visited 18 surveillance users at their premises in order to gain a thorough understanding of the way surveillance is used in public places in Victoria. Many of these users have surveillance technology in place that can record the images of thousands of people in a day. We viewed the technology used, discussed the individual practices of operators, and examined the protocols and procedures in place to protect the integrity of the information collected.
- 1.52 We conducted 32 consultations with users of surveillance, advocacy organisations, and experts seeking feedback on our proposed reform options.
- 1.53 As well as formal consultations, the commission hosted five forums with groups who experience public place surveillance, including young people, people experiencing homelessness, and culturally and linguistically diverse communities.⁴⁷

Consultative committee

- 1.54 In 2009 we established a consultative committee of individuals with different experiences of public place surveillance to gain responses to our draft recommendations. Although the committee members provided us with a lot of useful advice, the commission alone is responsible for the recommendations in this report.
- 1.55 The committee members were:
- Louise Connor, Secretary (Victoria), Media and Arts Alliance
 - Andy Frances, Manager, Security and Venue Support, Melbourne Cricket Club
 - Leigh Gassner, former Assistant Commissioner, Region 1 (CBD), Victoria Police
 - Moira Paterson, Associate Professor, Monash University Faculty of Law
 - Michael Pearce SC, President, Liberty Victoria
 - Bill Penrose, Vice President, Victorian Local Governance Association
 - Jen Rose, Manager, Policy and Projects, Youth Affairs Council of Victoria
 - Helen Versey, Victorian Privacy Commissioner
 - Dr Deane Wilson, Senior Lecturer in Criminology, Monash University.

OUTLINE OF THIS REPORT

- 1.56 The following chapter describes the major users of surveillance in Victoria and the purposes of their surveillance activities. In Chapter 3 we provide an overview of the current law relating to public place surveillance and highlight the inconsistencies and gaps in the legislative framework.
- 1.57 Chapter 4 discusses the benefits and risks of surveillance and the rights that may be affected by its use. When used responsibly, surveillance in public places can serve important and beneficial social purposes. The commission's recommendations aim to preserve these benefits while safeguarding against potential harm. This chapter also explains the commission's approach to regulatory reform.

- 41 Law Reform Commission of Hong Kong, *Privacy: The Regulation of Covert Surveillance Report* (2006).
- 42 *Interception of Communications and Surveillance Ordinance 2006* (Hong Kong) pt 2.
- 43 Law Reform Commission [Ireland], *Privacy: Surveillance and the Interception of Communications LRC 57-1998* (1998).
- 44 Ireland, Working Group on Privacy, *Report* (2006).
- 45 *Criminal Justice (Surveillance) Act 2009* (Ireland) ss 7, 8. *The Commission Publications Library*, The Law Reform Commission of Ireland <www.lawreform.ie/publications/publications.htm#TABLE_OF_Implementation_of_Commission_Re> at 12 January 2010.
- 46 Submissions are listed in Appendix A and reproduced at www.lawreform.vic.gov.au.
- 47 Forums, consultations and site visits and forums are listed in Appendix B.

Introduction

- 1.58 Chapters 5, 6 and 7 contain the commission’s recommendations for the regulation of surveillance in public places. The central focus is good advice about best practice. In Chapter 5 we explain our overarching principles that are designed to guide responsible use of public place surveillance by all users. We also detail one of our major recommendations—the creation of an independent regulator to inform and guide users about the practical implementation of these principles and advise the public about their operation.
- 1.59 Although appropriate guidance about the responsible use of surveillance in public places is a cornerstone of our recommendations, we do not believe that guidance alone can protect people from some practices that seriously affect their privacy. Chapters 6 and 7 deal with additional regulatory measures for particularly offensive uses of surveillance.
- 1.60 Although the SDA is the major piece of legislation that deals with public place surveillance it was not designed for this purpose. Its primary aim is to prohibit the use of covert surveillance devices in private places, while also allowing law enforcement agencies to use such devices with judicial authorisation. In Chapter 6 we recommend amendments to clarify, modernise and strengthen the SDA. These include refining some of the existing prohibitions and introducing a civil penalty regime.
- 1.61 In Chapter 7 we recommend the introduction of two statutory causes of action for serious invasions of privacy caused by misuse of surveillance devices in public places. The first deals with misuse of private information, the second with intrusion upon seclusion. We provide an overview of the current law in Australia and other comparable jurisdictions, and discuss matters of detail such as the elements, defences and remedies.

Chapter 2

Use of Surveillance in Public Places



CONTENTS

- 30 Introduction
- 31 Surveillance technology
- 32 Major users of public place surveillance
- 43 Conclusion

Use of Surveillance in Public Places

INTRODUCTION

- 2.1 This chapter examines the various forms of public place surveillance in Victoria, who uses it, and why.
- 2.2 There is no single comprehensive source of information about the use of public place surveillance in Victoria. Therefore, our description has been informed by the results of our discussions with users of public place surveillance and our examination of published research. In this chapter we list the major users of public place surveillance and describe their surveillance practices and the technologies used. The many important purposes served by public place surveillance—including safety, crime prevention and control, journalism and entertainment—are outlined in Chapter 4.
- 2.3 Government agencies and departments, individuals and private organisations of all sizes use public place surveillance extensively and its use is increasing. Victorians can expect to be observed, recorded and tracked while engaging in daily activities in our streets, shops and major public venues.
- 2.4 By far the most common form of surveillance is visual surveillance, particularly by the use of CCTV cameras. As systems are becoming cheaper and easier to install and use, CCTV is increasingly relied upon by government and private users. There is also growing use of other surveillance technologies, notably tracking devices, in Victoria. We provide definitions and descriptions of the various surveillance technologies in this chapter.
- 2.5 In our Consultation Paper we discussed some current trends in relation to surveillance use in Victoria. These are:
- the use of increasingly sophisticated technological devices with greater capacities
 - the decreasing cost of surveillance devices and their greater use by businesses and individuals
 - the increase in mass surveillance that 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.¹
- 2.6 There is also a tendency for technologies to converge, allowing for the creation of devices with increased surveillance capabilities. CCTV, for example, may be combined with facial recognition technology (described below) to identify individuals from their images. Another example is modern mobile phones, which combine telephonic services with GPS tracking software, digital visual and sound recording capabilities, and connection to the internet. A consequence of the convergence of surveillance technologies is the greater ability of surveillance users to compile detailed pictures of members of the public,² making it increasingly difficult for individuals to maintain their privacy and anonymity.³

SURVEILLANCE TECHNOLOGY

CLOSED-CIRCUIT TELEVISION (CCTV)

2.7 A CCTV system is one in which a number of video cameras are connected through a closed circuit or loop, and the images taken by these cameras are sent to a television monitor or recorder.⁴ The term 'closed circuit' highlights the private nature of the system and distinguishes it from television broadcasting from which anyone can receive signals.⁵ Increasingly, modern CCTV cameras use digital technology and are no longer closed circuit but are usually networked digital cameras.⁶ The expression CCTV is still commonly used, however, to refer to camera surveillance. Increasingly, CCTV is combined with software capable of 'smart' surveillance.⁷ For example, some CCTV systems can track individuals within a camera image or across multiple screens.⁸

GLOBAL POSITIONING SYSTEM (GPS) AND SATELLITE TECHNOLOGY

2.8 Many location devices rely on GPS technology. GPS works by measuring the time it takes a signal to travel the distance between a satellite and the device itself. GPS is commonly used in vehicles and handheld objects such as mobile phones⁹ and personal digital assistants. The nature of the technology means the device itself can be used as a tracking device.¹⁰

TRACKING MOBILE PHONES

2.9 Every mobile phone has an unchangeable electronic serial number (ESN), which, when combined with a phone number, makes the phone easily distinguishable by a telecommunications service provider, enabling the telephone to be tracked over time.¹¹ GPS applications on mobile phones mean that phones can also be used for location or tracking surveillance.¹²

RADIO FREQUENCY IDENTIFICATION (RFID)

2.10 RFID is another type of tracking device that enables identification of an object. The technology relies on a small transponder, known as a radio frequency tag, to transmit and receive radio signals to and from a scanner, known as a radio frequency reader.¹³ 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. A passive RFID tag is powered by an external source, for example the e-tag reader on Melbourne freeways. Although a passive RFID tag, such as the e-tag, cannot be used to monitor the location of a vehicle constantly, it will identify the tag, and therefore the vehicle, when it is near a reader. In this way this technology can, for example, be used to track a vehicle.

2.11 Another example of RFID as a surveillance device is the new public transport ticketing system myki, which uses RFID to allow access to transport. Cards that are not issued on an anonymous basis include details about the card holder. There is, therefore, the potential for card holders' movements to be tracked while using the transport system through the records of their card use.¹⁴

AUTOMATIC NUMBER PLATE RECOGNITION (ANPR)

2.12 Another technology that can be used for location and tracking surveillance is automatic number plate recognition (ANPR). ANPR uses a camera and optical character recognition software to locate a vehicle's number plate in an image of the vehicle and convert the number plate to text.¹⁵ The car's number plate can be matched to a car registration database to identify the car owner or other matters of interest.

- 1 See Victorian Law Reform Commission, *Surveillance in Public Places*, Consultation Paper 7 (2009) 26–36.
- 2 New Zealand Law Commission, *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1*, Study Paper 19 (2008) 136.
- 3 Kevin Haggerty and Richard Ericson, 'The Surveillant Assemblage' (2000) 51 *British Journal of Sociology* 605, 619.
- 4 Benjamin Goold, *CCTV and Policing* (2004) 12.
- 5 *Ibid* 12.
- 6 New Zealand Law Commission, *Privacy: Concepts and Issues*, above n 2, 140 citing Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* (2007) 33.
- 7 Tom Riley et al, 'Implementing Advanced Image Processing Technology in Sensor Systems for Security and Surveillance' *Proceedings of SPIE—The International Society for Optical Engineering: Volume 6741* (2007) 1, 3.
- 8 Anton van den Hengel, Anthony Dick and Rhys Hill, *Activity Topology Estimation for Large Networks of Cameras*, School of Computer Science, University of Adelaide <www.acvt.com.au/research/surveillance/AVSS06.pdf> at 1 October 2009.
- 9 In 2008, an estimated 10–20% of mobile phones had GPS: 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).
- 10 See eg, Telstra, *Whereis Everyone FAQ* <<http://everyone.whereis.com/home/faq/#faq26>> at 28 January 2010.
- 11 Recent Development, 'Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators' (2004) 18; *Harvard Journal of Law and Technology* 307, 309; Timothy Stapleton, 'The Electronic Communications Privacy Act and Cell Location Data: Is the Whole more than the Sum of its Parts?' (2007) 73; *Brooklyn Law Review* 383, 386.
- 12 Telstra, above n 10.
- 13 Privacy Commissioner [New Zealand], 'Tracking Technology on the Move' (2005) 54 *Private Word* 1.
- 14 Metlink, *Victorian Fares and Ticketing Manual (myki)* (2009) 43 <www.metlinkmelbourne.com.au/fares-tickets/victorian-fares-and-ticketing-manual-myki/> at 23 November 2009.
- 15 Crimtrac, *Automated Number Plate Recognition* <www.crimtrac.gov.au/systems_projects/AutomatedNumberPlateRecognitionANPR.html> at 11 November 2008.

Use of Surveillance in Public Places

BODY IMAGING DEVICES AND SCANNERS

- 2.13 Some types of body scanners have recently come into use at international airports in a number of countries. One type relies on x-ray technology, which has been used for over 100 years,¹⁶ most commonly for medical purposes. Recently, the Australian Government has trialled the use of body scan x-ray machines as an alternative to pat down checks to identify items such as weapons or explosives concealed beneath a passenger's clothing.¹⁷ Another type of body scanner that was trialled is the millimetre wave scanner, which uses very low-level radio waves (similar to a radar) to scan the human body. This creates an image that may also be used to detect objects concealed under an individual's clothing.¹⁸
- 2.14 Thermal imaging cameras work by detecting and measuring the heat radiating from an object or person. This type of technology has been used in Australian airports to identify individuals with higher than normal body temperatures that may indicate a person suffering from a particular virus, for example, swine flu.¹⁹
- 2.15 Another type of technology is the residue scanner used in some airports and prisons. It works by blowing air over an individual's body in order to release small particles attached to the skin, hair or clothing. The particles are analysed for trace amounts of explosives or drugs.²⁰

BIOMETRIC TECHNOLOGIES

- 2.16 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.²¹ An example of a biometric technology used in combination with camera surveillance is facial recognition technology, which compares a camera image of an individual's face with images held in a database to determine the individual's identity.

GOOGLE EARTH AND GOOGLE STREETVIEW

- 2.17 Google Inc., a publicly-listed US company specialising in internet search technologies and other web-based services, has developed two popular services using public place surveillance: Google Earth and Google Streetview. Google Earth is a free online database of satellite images that provides a bird's eye view of a location, searchable by landmark or address.²² Google Streetview provides a curbside view of streets and other locations. Vehicles with rooftop-mounted cameras capture images. This application is also free and is searchable by address or landmark. Streetview provides a higher level of clarity; in some cases it is possible to identify faces and other identifying features such as number plates. To address privacy concerns, these features may be blurred.²³

MAJOR USERS OF PUBLIC PLACE SURVEILLANCE

VICTORIA POLICE

- 2.18 Victoria Police has access to state-of-the-art surveillance technology and its use of surveillance devices in Victoria is extensive. Police routinely use optical surveillance, including stationary CCTV systems and hand-held devices, in relation to the investigation and prevention of crime. Cameras are also fitted to the front and rear of some metropolitan and regional police vehicles.²⁴ In some instances, video surveillance is coupled with software to enhance its capabilities. For example, the Victorian government recently announced its intention to provide funding for police use of facial recognition software to identify individuals.²⁵

- 2.19 Police also use listening devices that can be handheld or installed at specific locations. The commission was told that some police officers record conversations between themselves and members of the public for evidentiary purposes.²⁶ Police must obtain a warrant issued by a judge or magistrate to conduct covert surveillance of private activities and conversations, unless they are a party to that activity or conversation.²⁷
- 2.20 Potential suspects may also be tracked through their mobile phone²⁸ or by ANPR. In 2007 Victoria Police and VicRoads trialled the use of ANPR to record the details of vehicles potentially involved in traffic violations and other matters of interest.²⁹ By late September 2009, 316 526 plates had been scanned and 6079 offences detected.³⁰ Other less common methods of surveillance, such as drug and explosive-detection dogs, are also used.
- 2.21 Police are also increasingly using data provided by other Victorian bodies, including government departments, local councils, private organisations and individuals. In some cases this is provided on an ad hoc basis; in others, formal agreements are in place. The collection and subsequent use of these data frequently falls outside the regulatory regime designed to deal with police use of surveillance.
- 2.22 At least one police station has attempted to simplify the process of locating CCTV footage from local businesses by asking business owners to complete a form describing the CCTV systems they use.³¹ There are also some formal agreements in place concerning police access to surveillance footage between organisations that operate CCTV systems and Victoria Police.³²
- 2.23 Victoria Police also funds the Crime Stoppers Victoria program. Images (either captured by CCTV or provided by the public) are publicised in order to elicit information about potential suspected criminals.³³

- 16 NDT Resource Centre, *History of Radiography* <www.ndt-ed.org/EducationResources/CommunityCollege/Radiography/Introduction/history.htm> at 10 March 2010.
- 17 'Australian airport trials full body X-rays' *Herald Sun* (Melbourne), 2 October 2008 <www.heraldsun.com.au/lifestyle/health-science/airports-trial-full-body-x-rays/story-e6frfhjf-1111117642977> at 20 April 2010.
- 18 Site Visit 17.
- 19 ABC Radio National, 'Thermal Imaging at Airports to Check for Flu Fevers', *AM*, 1 May 2009 <www.abc.net.au/am/content/2008/s2557794.htm> at 28 January 2010.
- 20 *IonScan Sentinel II*, Global Security Solutions <www.global-security-solutions.com/IonScanSentinel.htm> at 13 October 2009.
- 21 New Zealand Law Commission, *Privacy: Concepts and Issues*, above n 2, 148.
- 22 *Google Earth Pro for Business Users*, Google <www.google.com/enterprise/earthmaps/earth_pro.html> at 14 January 2010.
- 23 *Street View FAQ*, Google <maps.google.com.au/help/maps/streetview/faq.html#howto_report_an_image> at 14 January 2010.
- 24 Victoria Police, 'First in Car Video Vehicles Launched' (Press Release, 25 July 2007) <www.police.vic.gov.au/content.asp?Document_ID=11796> at 28 January 2010.
- 25 Minister for Police and Emergency Services, 'Facial Recognition Technology will Catch Criminals' (Press Release, 30 April 2007).
- 26 Consultation 20.
- 27 *Surveillance Devices Act 1999* (Vic) ss 6, 7.
- 28 Police must obtain a warrant from a magistrate before undertaking this form of surveillance. *Surveillance Devices Act 1999* (Vic) s 8.
- 29 See Victoria Police, *Inquiry into Automatic Number Plate Recognition Technology* (2008) <www.parliament.qld.gov.au/view/historical/documents/committees/TSAFE/inquiry/ANPR%20technology/Submissions/14.pdf> at 14 January 2010.
- 30 'Vic Police Trial Hi-Tech Traffic Cameras', *The Age* (Melbourne), 5 September 2009 <<http://news.theage.com.au/breaking-news-national/vic-police-trial-hitech-traffic-cameras-20090905-fbo9.html>> at 28 January 2010.
- 31 Victoria Police, 'Wyndham Police Call Out to Local Businesses' (Press Release, 27 August 2008) <www.police.vic.gov.au/content.asp?Document_ID=16904> at 13 October 2009.
- 32 Consultation 22.
- 33 *Sharing Crime Information Online*, Crimestoppers <www.vic.crimestoppers.com.au/articleZone.aspx?articleZoneID=11> at 28 January 2010.



CORRECTIONS VICTORIA

- 2.24 Corrections Victoria also uses state-of-the-art surveillance technology. While much of its surveillance is not conducted in public places, Corrections Victoria does track some people in public places under a home detention scheme.³⁴ In some cases, individuals placed on a home detention order can engage in employment and some community activities but must wear a tamper-proof electronic tracking bracelet equipped with an active RFID tag that enables supervising officials to monitor the individual's location.³⁵ Before a home detention order can be granted, the offender must sign an undertaking consenting to be monitored in this way.³⁶
- 2.25 Since 2005 Corrections Victoria has also used a residue scanner in some prisons. This machine blows air over an individual to detect trace amounts of explosives and drugs. Iris scanning equipment was also introduced at the entry and exit of the Melbourne Assessment Prison in 2005.³⁷

LOCAL COUNCILS

CCTV

- 2.26 While the Victorian and federal governments fund some CCTV initiatives, local councils are the primary government user of CCTV throughout the state.³⁸
- 2.27 Melbourne City Council has the largest council-operated CCTV network in Victoria. The network has been in place since 1997,³⁹ and has had 54 cameras in operation since an upgrade of the system in 2009.⁴⁰ The cameras operate 24 hours a day, have the capacity to tilt and zoom, and can rotate 360 degrees. They are placed throughout the city, including in areas known to have high crime rates, and on some landmark buildings.⁴¹ The council also uses portable cameras for crowd control during major events. These are mounted on poles and removed within 24 hours.⁴² In addition, in 2009 the Melbourne City Council began trialling the use of two CCTV security vehicles that are installed with cameras that record a 360 degree view from the vehicle as it drives through the streets.⁴³
- 2.28 Melbourne City Council has established detailed protocols that govern its use of the CCTV system. These note the council's commitment to privacy and include procedures relating to security and access to footage, release of information and provisions for sharing some types of information with Victoria Police. An external consultant evaluates the policy every three years.⁴⁴ Council's use of CCTV is also subject to scrutiny by an audit committee made up of senior staff and external members. The committee provides oversight for council's operations, including storage, security, accuracy of documentation relating to CCTV footage and the provision of footage to Victoria Police.⁴⁵
- 2.29 A number of other metropolitan and regional councils also use CCTV cameras in central business districts and high-crime areas. The arrangements regarding the ownership and operation of systems vary between councils. One local council has established a partnership with an incorporated body (made up of local businesses owners and a councillor) to install CCTV systems in a shopping strip and other identified areas.⁴⁶ Footage from the systems is streamed live into the local police station and monitored by an officer on duty.⁴⁷ Procedures for the operation and management of the CCTV system are set out in guidelines agreed to by the incorporated body and Victoria Police. These stipulate that the incorporated body is responsible for all costs and liability arising from the operation of the CCTV cameras.⁴⁸

2.30 The commission is aware that there are a number of other models in place for the management of council systems. In one central business district council staff monitor footage from the central police station. Footage is monitored at busy times (ie weekend nights) and during special events only. Senior officers are involved in the training of council staff, and staff may contact police if they become aware of an incident occurring. Footage is also recorded and available for police viewing at any time.⁴⁹ Other councils contract security companies to operate their systems.⁵⁰

GPS

2.31 Local councils also use GPS to monitor activities within their council area. The media have reported that local councils have, for example, used GPS and Google Earth to 'check on illegal pools, buildings and vegetation clearing'.⁵¹ As long ago as 2001, at least one local council was using GPS to identify potential fire hazards on private residential property in its district.⁵²

PUBLIC HOUSING

2.32 The Housing and Community Building Division of the Department of Human Services is responsible for the wireless CCTV network in operation at high-rise public housing estates. The network was initially established to monitor equipment and manage maintenance issues, but has since been expanded to include camera surveillance. Cameras are located in lifts, foyers, car parks, plant rooms and on external walls. Some cameras are strategically placed in areas where criminal activity, such as drug dealing, may occur. Although the cameras are not hidden, there are no signs notifying people of their use. In some instances covert cameras have been installed upon police request when there has been a strong suspicion of criminal activity.⁵³

2.33 All CCTV footage is fed to an offsite control room monitored by a contracted security company. At larger housing estates there are also onsite control rooms and security staff who monitor footage in real time. Footage is stored at the central control room for 28 days and at the onsite control rooms for five days. Cameras that are able to pan, tilt and zoom can be manoeuvred by onsite security personnel and by staff at the central control room.⁵⁴

UNIVERSITIES AND TAFES

2.34 The commission consulted Victorian universities in our preliminary consultation period. All universities consulted by the commission use CCTV to monitor their campuses for the purpose of protecting students, staff and property. Some institutions use surveillance cameras to monitor the movements of any individual on the campus late at night. All universities and TAFEs the commission consulted have internal policies regarding the storage, access and use of footage obtained by CCTV.⁵⁵

2.35 Universities and TAFEs can also track student and staff movements through their university identity cards. These cards hold information about users and provide access to particular campus locations, which enables individuals who have used the card to be potentially located or subsequently tracked.⁵⁶

TRANSPORT

2.36 Transport operators rely heavily on surveillance technologies—including visual, audio and tracking devices. Specific uses are outlined below.

34 Approximately 35–50 people are subject to home detention every year in Victoria: Melbourne Centre for Criminological Research and Evaluation for Corrections Victoria, Department of Justice, *Home Detention in Victoria: Final Evaluation Report* (2006) 8.

35 *Home Detention*, Department of Justice (Vic) (2008) <www.justice.vic.gov.au/wps/wcm/connect/DOJ+Internet/Home/Sentencing/Home+Detention/> at 28 January 2010.

36 *Surveillance Devices Act 1999* (Vic), s 8(1)(a); *Corrections and Sentencing Acts (Home Detention) Act 2003* (Vic), s 18ZZ(1)(b).

37 Selma Milovanovic, 'Blown Away by New Technology', *The Age* (Melbourne), 30 December 2005, 4.

38 Adam Sutton and Dean Wilson, 'Open-Street CCTV in Australia: The Politics of Resistance and Expansion' (2004) 2 *Surveillance and Society* 310, 313.

39 Site Visit 5.

40 *Safe City Cameras*, City of Melbourne <www.melbourne.vic.gov.au/CommunityServices/CommunitySafety/Pages/SafeCitycameras.aspx> at 28 January 2010.

41 Site Visit 5.

42 Consultation 10.

43 Jason Dowling, 'CCTV Security Vehicles to Patrol CBD Streets', *The Age* (Melbourne), 10 November 2009 <www.theage.com.au/national/cctv-security-vehicles-to-patrol-cbd-streets-20091110-i6e8.html> at 28 January 2010.

44 Consultation 10.

45 Site Visit 5.

46 Consultation 22.

47 Consultation 22.

48 Lilydale Centre Safe Committee Incorporated, Lilydale (2006) *Memorandum of Understanding between Lilydale Centre Safe Committee Incorporated, Lilydale and Victoria Police*, provided by Victoria Police 12 February 2010.

49 Consultation 27.

50 Jeff Jones, 'CCTV for Dandenong North Shops', *The Dandenong Leader*, 12 October 2009 <<http://dandenong-leader.whereilive.com.au/news/story/cctv-for-dandenong-north-shops>> at 12 March 2010; Consultation 10.

51 Lachlan Heywood, 'Public Told not to Fear Council Spies in the Sky', *The Courier Mail* (Brisbane), 19 September 2003, 18.

52 Sue Cant, 'Satellites Help Council Spot Fire Hazards', *The Age* (Melbourne), 16 January 2001, 2.

53 Site Visit 18.

54 Site Visit 18.

55 Roundtable 10.

56 Roundtable 10.



Trains

- 2.37 CCTV is used in and around metropolitan and regional train stations for a number of purposes, including monitoring train movements, passenger safety, and deterring and investigating crime. The number of cameras at a particular station can be significant—Flinders Street Station, for example, has approximately 150 cameras and Southern Cross Station 180, all operating 24 hours a day. Most cameras show only a fixed view and only a few have zoom, pan and tilt functions. Some stations erect signs notifying of the surveillance.⁵⁷
- 2.38 Cameras operate inside most train carriages on metropolitan train lines.⁵⁸ Footage cannot be viewed from train stations but can be viewed by the driver. When a duress alarm sounds in a carriage, the driver is alerted to the view in that carriage.⁵⁹
- 2.39 At larger stations the station’s footage is monitored from an onsite control room;⁶⁰ on suburban lines footage for several stations is monitored from a central suburban station.⁶¹ Control room operators and Department of Transport personnel can view footage live, but do not have access to recorded footage; recorded footage from cameras at train stations and inside trains is accessible only to management centre staff.⁶² The commission was told that police requests for footage was increasing. There is a formal process within the department for dealing with all requests for footage.⁶³
- 2.40 Myki, the new public transport ticketing system, uses passive RFID in plastic cards to allow access to transport. The myki system ‘will provide passengers with smart travel cards that can calculate and automatically deduct fares from pre-paid accounts’.⁶⁴ Except when issued on an anonymous basis, use of these cards could potentially enable a person’s movements through the transport system to be tracked and recorded.⁶⁵

Trams

- 2.41 CCTV is used for operational and safety purposes on the Melbourne metropolitan tram network. For example, footage from VicRoads traffic control cameras is provided to Yarra Trams to monitor traffic conditions.⁶⁶ Specific incidents can be highlighted to better enable staff to monitor and manage incidents. CCTV also operates on board newer Melbourne trams.⁶⁷ These cameras are mounted on the front and sides of trams and, in a bid to improve passenger safety, capture images of cars that illegally drive past stationary trams.⁶⁸
- 2.42 GPS tracking devices have also been installed in trams to allow trams to be tracked in real time and for information to be relayed to passengers waiting at tram stops.⁶⁹ The tracking system also communicates with VicRoads to ensure that trams are given priority at certain intersections across Melbourne.⁷⁰ Trams can also be tracked by individuals through an iPhone application.⁷¹

Buses

- 2.43 Some metropolitan buses have CCTV cameras that capture images inside buses. These generally record while the bus is in operation. More modern buses also have sound recording capabilities that record while the bus is in operation. Footage and recordings may be reviewed at a later date in relation to a specific incident. Some buses display signs notifying of surveillance.⁷² GPS tracking systems are also used on some metropolitan bus routes. The information is used by VicRoads to request priority at traffic lights and to provide accurate wait times at bus stops.⁷³

Taxis

- 2.44 All taxis that operate in the metropolitan, outer-suburban and Geelong taxi zones are required by law to have cameras installed to capture images inside the vehicle. Taxis must display notices inside and outside the taxi to notify of the presence of the cameras.⁷⁴ Footage can be viewed only by transport safety officers. Footage may be released to a driver or passenger only in relation to an incident reported to police and upon written request from a police officer.⁷⁵
- 2.45 Approximately 90 per cent of Victorian taxis have GPS installed. In addition to assisting drivers to determine which route to follow, the system can also assist in emergencies. Once a driver triggers a duress alarm, the base operators can track the vehicle. A one-way voice channel is also activated so that the conversation inside the taxi can be heard at base.⁷⁶
- 2.46 Some local councils have established taxi ranks at which a customer's identification information is collected and photo identification may be scanned.⁷⁷ Privacy Victoria has expressed concern regarding the privacy implications of this practice and as a result some local councils have abandoned it.⁷⁸

Roads

Cameras

- 2.47 There are between 600 and 700 cameras used to monitor and manage traffic on Victoria's roads, including cameras owned by VicRoads and private toll road operators Citylink and Eastlink. The majority of these cameras can be tilted and zoomed. VicRoads and private operators continuously monitor footage from inhouse control rooms.⁷⁹ VicRoads has at least two operators in a control room at all times. Once alerted to an incident or traffic situation, operators use cameras to determine an appropriate traffic management response.⁸⁰
- 2.48 VicRoads generally does not record footage. Where footage is recorded, it is usually for operational purposes such as reviewing the effectiveness of a change in a traffic management plan. There are no signs notifying the public that cameras are in operation.⁸¹
- 2.49 Footage can be provided to Victoria Police if requested for criminal investigations. CityLink also provides real-time webcam images of major Melbourne roads on its website in order to enable individuals to view traffic conditions.⁸² VicRoads is considering the use of similar webcams.⁸³

Tracking devices

- 2.50 Toll collecting systems on Citylink and Eastlink use RFID technology in e-tag transponders for billing and payments. When a car carrying an e-tag passes a reader on the freeway, a fee is automatically charged to the individual's account without the car having to stop. If no e-tag registers as a vehicle passes, cameras are triggered to capture images of the front and the back of the vehicle. The information is downloaded and optical character recognition software is used to read and record licence plate details. In most situations a toll is automatically charged.⁸⁴
- 2.51 Where photographs do not provide a clear image, an operator will review the footage to determine the licence details and may contact VicRoads for registration details for billing purposes.⁸⁵ VicRoads also uses fixed and mobile cameras with ANPR technology to detect traffic infringements such as running red lights and speeding.⁸⁶

- 57 Site Visits 2, 4.
- 58 The commission was informed in a 2007 Roundtable consultation that regional train services do not have internal CCTV because these are staffed by conductors: Roundtable 3.
- 59 Site Visit 4.
- 60 Site Visits 2, 4.
- 61 Site Visit 4.
- 62 Site Visit 4.
- 63 The Department of Transport process for determining police requests for footage is known as the 'Keeper of Evidence' process. See Site Visit 4.
- 64 *How Will I Use Myki?*, myki <www.myki.com.au/use-myki_your-key.aspx> at 12 November 2008.
- 65 Metlink, above n 14.
- 66 Yarra Trams, 'Think Tram Takes a Closer Look at the Tram Network' (Press Release, 3 February 2009) <www.yarratrams.com.au/desktopdefault.aspx?tabid-105/99_read-1748/> at 28 January 2010.
- 67 Stephen Moynihan, 'Stop! Tram-Stop Sneaks will be in the Picture', *The Age* (Melbourne), 2 July 2007 <www.theage.com.au/news/national/snap-tramstop-sneaks-targetted/2007/07/01/1183228960462.html?s_cid=rss_age> at 28 January 2010.
- 68 Ibid.
- 69 *Think Tram Projects*, VicRoads <www.vicroads.vic.gov.au/Home/PublicTransportAndEnvironment/PublicTransportOnRoads/TramProjects/ThinkTramProjects.htm> at 14 January 2010.
- 70 Ibid.
- 71 Clay Lucas, 'iPhone App Tracks Tram in Real-Time', *The Sydney Morning Herald* (Sydney), 15 June 2009 <www.smh.com.au/digital-life/mobiles/iphone-app-tracks-trams-in-realttime-20090615-c8ut.html> at 28 January 2010.
- 72 Forum 3.
- 73 *SmartBus Infrastructure*, Department of Transport (Vic) <www.transport.vic.gov.au/web23/Home.nsf/AllDocs/90A14F13EABE24E4CA25766600140C50?OpenDocument> at 28 January 2010.
- 74 Submission 3, Victorian Taxi Directorate, *Function and Performance Specification for a Taxi Safety Camera System 2009* (2009).
- 75 Site Visit 8.
- 76 Site Visit 8.
- 77 Office of the Victorian Privacy Commissioner, *Annual Report 2008–2009* (2009) 12; *Photo Identification Scheme for Geelong Taxis* (2008) ABC News <www.abc.net.au/news/stories/2008/06/16/2275860.htm> at 14 January 2010.
- 78 Office of the Victorian Privacy Commissioner, above n 77, 12.
- 79 Site Visit 1.
- 80 Site Visit 9.
- 81 Site Visit 1.
- 82 See Citylink <www.citylink.com.au> at 28 January 2010.
- 83 Site Visit 1.
- 84 Site Visit 9.
- 85 Site Visit 9.
- 86 Site Visit 1.



Monitoring heavy vehicle movements

- 2.52 Heavy freight vehicles are restricted from using some roads because their size and mass can damage infrastructure or threaten safety. The Intelligent Access Program (IAP) is a voluntary program that allows controlled vehicles access to additional roads on the condition they install a GPS monitoring device and allow tracking by the Transport Certification Authority. In 2009 over 3000 vehicles voluntarily registered for involvement in the IAP across Australia.⁸⁷

Airports

- 2.53 Airports use a number of surveillance technologies. For example, since 2005 all Australian passports have included embedded RFID chips⁸⁸ that can be read by an airport scanner. The chip contains information that includes the holder's photograph, name, signature, gender, date of birth, passport number and expiry date.⁸⁹
- 2.54 In 2008 the SmartGate system was introduced at Melbourne international airport.⁹⁰ The system, which relies on facial recognition technology, enables Australian and New Zealand citizens to process themselves through passport control.⁹¹ If the machine does not detect a match, the individual must go through manual processing with a customs official.⁹²
- 2.55 In 2008 the federal government trialed the use of x-ray and millimetre-wave body scanning systems at Melbourne, Sydney and Adelaide airports.⁹³ These scanners were used as an alternative to a pat-down search to see through passenger clothing to determine whether items such as weapons or explosives had been concealed. In February 2010 the federal government released plans to install x-ray body scanners in international airports as part of increased security measures.⁹⁴
- 2.56 Another technology sometimes used in airports is thermal imaging, which is used to identify people with higher than normal body temperatures.⁹⁵ In 2009, thermal imaging machines were installed in Australian international airports to detect passengers arriving from overseas who may have had the swine flu virus.

Port of Melbourne

- 2.57 The Port of Melbourne Authority operates 180 CCTV cameras to maintain employee health and safety and to protect against crime, including theft and terrorist acts. Some cameras are positioned around bulk liquid terminals; others overlook the beach and the pier. Footage is relayed to a central control room and is continuously monitored by contracted security personnel. Footage is also provided to the Water Police. There are no signs notifying the public of the use of surveillance cameras in the area.⁹⁶

MAJOR PUBLIC EVENTS: CONCERTS AND SPORTS

- 2.58 The commission consulted with two major sporting venues in Melbourne: Etihad Stadium (Etihad) and the Melbourne Cricket Ground (MCG). Both rely heavily on surveillance technology for the management of crowds, the protection of people and property, and for responding to claims about injuries sustained at the venue.⁹⁷
- 2.59 The MCG, which holds approximately 100 000 people, has 400 cameras in operation.⁹⁸ Etihad is much smaller, with a capacity of 58 000 people and 63 cameras.⁹⁹ Both organisations are considering upgrading their systems in the near future. Some cameras pan the crowd and several monitor the perimeter of the premises. A powerful camera is used by the MCG to monitor crowd flow from nearby train stations and traffic flow outside the MCG. It can zoom up to 1.5 kilometres.¹⁰⁰ There are signs in both stadiums notifying patrons of the use of these systems.¹⁰¹

- 2.60 On event days security staff and police officers operate the control rooms. The police have a leading role in directing camera operation.¹⁰² Footage is recorded and stored for up to 30 days.¹⁰³ The MCG's policy is to release footage only to police, insurers, and in response to a subpoena or court order. When members of the public request footage a court order is requested.¹⁰⁴ To date Etihad has not received a request for footage from a member of the public but suggested that if it did, it would probably refer the matter to the police.¹⁰⁵
- 2.61 Other security measures used at the MCG include the use of a duress alarm by cashiers. The alarm is linked to the CCTV system. Pressing the alarm button will ensure that the camera records and retains footage from 15 seconds before the alarm was activated. The MCG also uses biometric fingerprint scanning for the purpose of controlling contractors' access to the ground.¹⁰⁶
- 2.62 The Melbourne Sports and Aquatic Centre (the Centre) is another major user of surveillance. The Centre operates 86 cameras across its premises, although not in change rooms and toilets. Footage can be viewed in the surveillance control room and the Duty Manager's office, although neither is continuously monitored. Footage, which is routinely viewed for safety purposes, includes monitoring the number of people using the pool and the location of staff. Recorded footage is also used to investigate criminal offences, including break-ins and theft. Signs notifying people that cameras are in operation are strategically placed to deter criminal activity.¹⁰⁷
- 2.63 The Centre stores footage for approximately 14 days after it is recorded and provides footage to the police upon request. The Centre has not received any requests for footage from members of the public and stated that if it did, it would be unlikely to provide it.¹⁰⁸

CROWN CASINO

- 2.64 Melbourne's Crown Casino (the Casino), which employs approximately 6000 staff, is visited by over 30 000 people every day. Crown Casino has one of the most advanced, complex and comprehensive video surveillance systems currently in use in Victoria. The primary component of this system is CCTV.¹⁰⁹
- 2.65 The Casino has an inhouse surveillance technical team that is responsible for maintaining the equipment, sourcing new equipment and keeping up to date with technology. As well as performing those general duties these staff are also responsible for developing inhouse surveillance technologies to suit the Casino's needs.¹¹⁰
- 2.66 In the past five years Crown Casino's CCTV system has undergone technological improvement, particularly in relation to the resolution quality of images and its digital recording capabilities. The Casino relies on the system to identify and prevent illegal activity, monitor cash handling and gambling activities, and to ensure patron and staff safety by responding quickly to incidents as they arise.¹¹¹
- 2.67 The Casino operates a large number of cameras within its premises. Many of the cameras have the capacity to pan, tilt and zoom. Often several cameras target one area, such as a gaming table. Some cameras are equipped with both audio and visual recording capabilities. There are others that begin recording only when motion is detected in a given area. In premium gaming rooms there is additional surveillance. In most of these areas access is restricted either by use of swipe cards or by a licensed officer at the door.¹¹²

- 87 Consultation 2.
- 88 *The Australian ePassport* (2009) Department of Foreign Affairs and Trade <www.dfat.gov.au/dept/passports/> at 28 January 2010.
- 89 Ibid.
- 90 *New Smartgate Technology at Melbourne Airport* (2008), Melbourne Airport <www.melbourneairport.com.au/About-Melbourne-Airport/Media/Media-releases/Media-Release-Archive/2008/NEW-SMARTGATE-TECHNOLOGY-AT-MELBOURNE-AIRPORT.html> at 28 January 2010.
- 91 Peter Hawkins, 'Sydney Airport Opens SmartGate', *Sydney Morning Herald* (Sydney), 27 September 2009 <www.smh.com.au/travel/travel-news/sydney-airport-opens-smartgate-20090926-g742.html> at 28 January 2010.
- 92 ABC Radio, 'New Airport Security System Tested in Sydney', *The World Today*, 29 January 2003 <www.abc.net.au/worldtoday/stories/s772230.htm> at 28 October 2009.
- 93 'Australian airport trials full body X-rays', above n 17.
- 94 Anthony Albanese MP, Minister for Transport, 'Strengthening Aviation Security' (Press Release, 9 February 2010).
- 95 ABC Radio National, 'Thermal Imaging at Airports to Check for Flu Fevers', *AM*, 1 May 2009 <www.abc.net.au/am/content/2008/s2557794.htm> at 28 January 2010.
- 96 Roundtable 10.
- 97 Site Visits 6, 14.
- 98 Site Visit 14.
- 99 Site Visit 6.
- 100 Site Visit 14.
- 101 Site Visits 6, 14.
- 102 Site Visit 14.
- 103 Site Visits 6, 14.
- 104 Site Visit 14.
- 105 Site Visit 6.
- 106 Site Visit 14.
- 107 Site Visit 12.
- 108 Site Visit 12.
- 109 Site Visit 13.
- 110 Site Visit 13.
- 111 Site Visit 13.
- 112 Site Visit 13.

Use of Surveillance in Public Places



- 2.68 A number of staff continuously monitor the CCTV system. The cameras are monitored in real time but footage can also be viewed retrospectively. The Casino's Security Communications Centre and the Victorian Commission for Gambling Regulation can also access surveillance footage in real time.¹¹³
- 2.69 Crown Casino has installed software that is used in conjunction with some of its cameras for surveillance purposes. For example, people-counting technology (which does not identify individuals) is used in conjunction with tracking software to determine the number of people entering the Casino. The Casino has also conducted trials of facial recognition technology but has found it to be of limited use.¹¹⁴
- 2.70 Crown Casino's nightclubs use identification scanning technologies at their entrances to record the details of the patrons entering. The use of this technology has assisted police to apprehend at least one serious offender. Police often alert the Casino to people who are of interest to their investigations. The identity scanner can be used in conjunction with CCTV to identify such individuals and monitor their movements.¹¹⁵

THE HOSPITALITY INDUSTRY

- 2.71 CCTV is widely used in the hospitality industry. Some licensed venues must have CCTV cameras that operate to proscribed standards and security staff as a condition of their licence,¹¹⁶ while other licensed venues choose to have security cameras even though it is not a condition of their licence. In addition to cameras within the premises, some venues also have cameras to view adjacent areas, such as footpaths and carparks. Footage from these cameras can be viewed in real time for crowd control purposes and to prevent criminal behaviour, and can also be viewed later to investigate crime. In early 2009 some interstate hospitality venues trialled the use of small cameras worn by security staff that record sound as well as pictures.¹¹⁷
- 2.72 Some nightclubs operate other forms of surveillance, including identification scanners and facial recognition technology.¹¹⁸ Identification scanners record the image and written details on an individual's driving licence or other identity card, including their name and address.¹¹⁹ Facial recognition software scans patrons' faces as they enter the nightclub and matches those images against a database of photos. In this way the software can be used to identify patrons who have been previously banned from a venue.¹²⁰ The software can be shared among venues.

SHOPPING CENTRES AND RETAILERS

- 2.73 Many shopping centres and retail outlets such as service stations, supermarkets and department stores rely on CCTV for crime prevention and detection.¹²¹ Large shopping centres typically use sophisticated CCTV systems that have many cameras operating both inside and outside the centre. Cameras tend to be concentrated on entrances and areas where there have been crime problems. One consultation participant mentioned that as handbag theft was especially common in food courts, there are more cameras in these areas.¹²² Service stations use CCTV to deter theft and record the details of individuals who leave the service station without paying for petrol so they can be provided to police.¹²³ One large shopping centre reported that its security personnel carry CCTV-captured images of people who have been banned from the centre so they can be identified and removed.¹²⁴

- 2.74 RFID tracking is also used by some businesses for stock control. In this system, a tag is attached to a pallet when it leaves the manufacturer and a scanner reads it at each stage of its journey to the distribution centre.¹²⁵ Some large retail chains are considering attaching RFID chips to individual boxes or items so they can be tracked to the store.¹²⁶
- 2.75 Passive RFID devices are also used as anti-theft mechanisms in many clothing and department stores. A tag on a garment triggers an alarm if the item is taken past readers that are usually situated at the entrance of the store. As a rule, tags can only be removed by the use of a device at the point of sale.

THE MEDIA

- 2.76 Media organisations use various surveillance devices in public places in order to carry out news gathering. For example, media organisations routinely use cameras and audio devices to record events and interviews. Unlike many organisations the media's use of surveillance does not generally occur on an ongoing basis in only one place, but typically for a short time in a given location.
- 2.77 Sometimes media organisations receive CCTV footage of alleged criminal conduct from third parties. This occurred in relation to the shooting in Melbourne's CBD in June 2007.¹²⁷ Generally, media organisations will attempt to corroborate such footage and will be careful to consider its likely authenticity.¹²⁸
- 2.78 Media groups told us they generally use surveillance equipment in an overt and obvious way.¹²⁹ When, for example, a news crew from a television station arrives at the scene of an event it is usually in a marked vehicle, with crew wearing clothing and carrying equipment marked with the logo of the television station.¹³⁰

MARKETING COMPANIES

- 2.79 Some organisations use surveillance technologies for marketing purposes. One example uses mobile phones with Bluetooth functionality. Location-based services detect that a phone is in a certain vicinity (for example, a shopping centre) and, at the customer's request, send information about nearby services.
- 2.80 The same process is also used for advertising.¹³¹ A Bluetooth transmitting device is placed in a location near a retailer or institution wanting to advertise to people nearby. The device sends a message to all Bluetooth-enabled mobile phones within 100 metres of the device and the mobile phone user either accepts or declines the offer from their phone.¹³² For example, pubs and clubs can advertise drink specials or cinemas can send people the latest movie session times.¹³³

PRIVATE INVESTIGATORS

- 2.81 Private investigators routinely engage in public place surveillance to carry out their work. While insurance companies are the primary source of work for private investigators, private clients also request investigations about matters such as matrimonial and child support issues. Footage is usually obtained in a covert manner, for example, from inside cars or from public places using concealed cameras. The commission was informed that toilets, change rooms, homes and private yards are considered no go areas for surveillance by private investigators.¹³⁴
- 2.82 Private investigators must hold a licence. An application for a licence must include details of the applicant's qualifications and any training or experience relevant to each private activity to be authorised under the licence.¹³⁵

- 113 Site Visit 13.
 114 Site Visit 13.
 115 Site Visit 13.
 116 Consultation 6; *Liquor Control Reform Regulations 1999* (Vic).
 117 Jacqui Jones, 'Little Camera a Big Deterrent', *The Herald* (Sydney), 23 February 2009 <www.theherald.com.au/news/local/news/general/little-camera-a-big-deterrent-in-late-night-violence/1440566.aspx#> at 28 January 2010.
 118 Consultation 27; Site Visit 10.
 119 Site Visit 10.
 120 Site Visit 10.
 121 Consultations 1, 7.
 122 Consultation 1.
 123 Consultation 7.
 124 Consultation 1.
 125 Teresa Scassa et al, 'Consumer Privacy and Radio Frequency Identification Technology' (2005-6) 37 *Ottawa Law Review* 215, 219.
 126 Consultation 16.
 127 Consultation 12.
 128 Consultations 12, 14.
 129 Consultations 12, 14.
 130 Consultation 12.
 131 Submission 19.
 132 *How It Works*, Bluetooth Advertising <www.bluetoothadvertising.com.au/how_it_works.html> at 28 January 2010.
 133 *Examples*, Bluetooth Advertising <www.bluetoothadvertising.com.au/examples.html> at 28 January 2010.
 134 Consultation 31.
 135 *Private Security Regulations 2005* (Vic) reg 13.

Use of Surveillance in Public Places



PUBLIC AND PRIVATE INSURERS

- 2.83 Public and private insurers hire private investigators to engage in some public place surveillance in order to determine the validity of some insurance claims.¹³⁶ The surveillance might include, for example, the use of an optical recording device in a public location, such as a park, to record the claimant's behaviour in order to test the truth of his or her statements.¹³⁷
- 2.84 The commission was told that while the use of covert surveillance is an important part of the insurance industry's ability to investigate claims, it is not a particularly common activity.¹³⁸ Private insurance companies advise policy holders in their disclosure statements that surveillance may be used to assess the veracity of any claim and to investigate possible fraud.¹³⁹

THE PRIVATE SECURITY INDUSTRY

- 2.85 Many surveillance systems in Victoria are managed and monitored by private security companies. The commission met a number of organisations (including government departments, local councils and private organisations) that outsource all or part of their security needs to private security firms.¹⁴⁰ There are many different arrangements. Some private security companies manage operations from their own premises using their own equipment (often for a number of clients) and others work at the venue itself under direction of venue staff. In contrast, some other organisations employ inhouse security staff to manage their operations.¹⁴¹
- 2.86 Contracted security personnel are required to undergo training,¹⁴² which must be provided by a registered training organisation at Certificate II or Certificate III level.¹⁴³ A Certificate III course typically takes three to four weeks to complete.¹⁴⁴ Some people we consulted raised concerns that, in contrast, inhouse security staff are not required to have any certification or training.¹⁴⁵

AGED CARE

- 2.87 RFID and GPS technology is used as a method to monitor the location of aged care patients suffering from dementia and other memory-affecting conditions. Alzheimer's Australia recommends that carers consider the use of a tracking device to monitor a person with dementia so that the individual can freely go for walks on their own but are also easily located if they become lost or disoriented. A device can be worn around the wrist, waist or neck. Some devices can be activated only by the person wearing the device, while others enable an external party to monitor the whereabouts of the person wearing the device.¹⁴⁶

PERSONAL USES

- 2.88 Individuals use surveillance devices in public places for a number of reasons. Optical surveillance devices, such as cameras and video recorders, are commonplace. The Victorian Association of Photographic Societies noted in its submission that photographers frequently use photography for legitimate purposes.¹⁴⁷
- 2.89 It is also now possible for individuals to track each other. Telstra, for example, offers a service that locates any Telstra mobile phone and marks the approximate address on an online map.¹⁴⁸ Although this service can be used only with the consent of the phone user and the person receiving the alert, there are other covert phone tracking services offered in Australia. One Sydney-based company offers 'mobile phone monitoring software' that can be downloaded onto a mobile phone without notification to the owner and can covertly copy, record and send to another account all communications made to and from that phone.¹⁴⁹ This type of service has been marketed, for example, to people to monitor their spouse. There have also been newspaper reports of an increasing number of parents tracking their children, including by mobile phone tracking systems.¹⁵⁰

- 2.90 The commission was also told about the importance of surveillance technologies in family disputes.¹⁵¹ Family violence victims, for example, have used covert surveillance to document abuse.¹⁵² Another group of individuals who routinely use surveillance devices are people involved in protests. Visual recording is used by activists 'where there are community concerns that violence may occur'.¹⁵³
- 2.91 There are some reports of individuals using surveillance for criminal purposes. There have been several cases of people using hidden cameras to record images up the skirts of unsuspecting women.¹⁵⁴ This practice, known as 'upskirting', is now a specific criminal offence.¹⁵⁵ Another disturbing use of surveillance devices by individuals is the practice of recording violent attacks on mobile phones and then distributing that footage. This practice, known as 'happy slapping', is discussed in greater detail in Chapter 4.
- 2.92 Surveillance in public places can also be used to facilitate other crimes. For example, covert surveillance cameras have been installed at ATMs to capture PIN numbers for the purpose of stealing from individual accounts.

CONCLUSION

- 2.93 Because public place surveillance is widespread in Victoria, we can no longer assume that activities performed in public places will pass unobserved and unrecorded. Government, private organisations and individuals are all extensive users of public place surveillance. Although there are many different practices, we found some common themes.
- Many agencies and organisations use CCTV. Although most systems can record large amounts of data, many are not actively monitored.
 - The sophistication of modern CCTV systems is increasing rapidly, including considerable pan, tilt and zoom capabilities, and an ability to film in colour or use an infrared light.
 - Contracted security companies are responsible for monitoring many of the CCTV systems that are actively monitored.
 - Because many cameras are small and are often placed in obscure positions, and because not all users of CCTV erect signs, it is likely that many people do not know that their image is being recorded as they go about their daily lives.
 - Smart surveillance, such as facial recognition technology, is not yet in widespread use.
 - In general, surveillance users appear to avoid private areas, such as toilets and change rooms.
 - Surveillance data, such as CCTV footage, is generally shared only with police and insurers.
 - While some organisations have good internal policies concerning their use of surveillance equipment, others do not.

- 136 Consultation 31.
- 137 Submission 16.
- 138 Submission 16.
- 139 Submission 16.
- 140 See eg, Consultation 10; Site Visits 15, 18.
- 141 See eg, Site Visits 1, 9, 12, 16.
- 142 Consultation 17.
- 143 Eg, the International Security Training Company offer a Certificate III in Security Operations (control room operator).
- 144 Consultation 18.
- 145 Consultations 17, 18.
- 146 Alzheimer's Australia, *Safer Walking for People with Dementia: Approaches and Technologies*, Update Sheet 16 (April 2009) 3, 4.
- 147 Submission 15.
- 148 Telstra, above n 10.
- 149 Mark Russell, 'I'll Be Watching You: Warning on Mobile Phone Tracking', *The Age* (Melbourne), 8 March 2009; Spousebusters, *Latest News* (2008) <www.hotfrog.com.au/Companies/Spousebusters/FullPressRelease.aspx?id=15557> at 11 March 2009.
- 150 'Parents Using Private Investigators on Kids', *The Advertiser* (Adelaide), 2 December 2009 <www.news.com.au/national/parents-use-private-investigators-on-kids/story-e6frfkvr-1225805939625> at 28 January 2010.
- 151 Submissions 14, 34, 40.
- 152 Submission 40.
- 153 Submission 34.
- 154 For recent examples see: 'Man Charged Over "Upskirting" Photos', *Sydney Morning Herald* (Sydney), 6 September 2009 <www.smh.com.au/national/man-charged-over-upskirting-photos-20090906-fccu.html> at 28 January 2010; Karen Matthews, 'Upskirting Case Delayed', *Geelong Advertiser* (Geelong), 24 September 2009 <www.geelongadvertiser.com.au/article/2009/09/24/106781_news.html> at 28 January 2010.
- 155 *Summary Offences Act 1966* (Vic) div 4A.

Chapter 3 Current Law

WARNING
PREMISES UNDER
CONSTANT
SURVEILLANCE

CONTENTS

- 46 Introduction
- 46 Surveillance devices legislation
- 47 Information privacy legislation
- 50 Regulation of specific aspects of public place surveillance
- 51 Common law protections
- 51 The Victorian Charter of Human Rights and Responsibilities
- 52 Non-binding guidelines, standards and policies
- 53 Regulation in other jurisdictions
- 54 Conclusion
- 55 Table 1: Legislation and binding codes relating to public place surveillance in Victoria
- 57 Table 2: Major non-binding instruments relating to public place surveillance in Victoria

INTRODUCTION

- 3.1 Most public place surveillance in Victoria takes place without any regulation. Although some of the most offensive forms of surveillance are prohibited, the two main relevant bodies of law—the *Surveillance Devices Act 1999* (Vic) (SDA) and Commonwealth and Victorian privacy laws¹—have limited application to public place surveillance. While some businesses, such as licensed venues, taxis and casinos, operate under industry specific laws that regulate their use of surveillance, these laws are not consistent. The result has been piecemeal regulation. This chapter outlines the regulatory regime governing surveillance in public places and highlights the gaps in the law. Table 1, on page 55, sets out all legislation relating to public place surveillance in Victoria.

SURVEILLANCE DEVICES LEGISLATION

- 3.2 The SDA was enacted in 1999 to replace listening devices legislation and to address the increasing use of different forms of surveillance, such as visual surveillance and tracking devices. When introducing the Act to parliament, the Attorney-General noted that it was designed to provide ‘stringent safeguards to protect individual privacy’.²
- 3.3 The SDA prohibits some uses of four types of surveillance devices: listening devices, optical surveillance devices, tracking devices and data surveillance devices. The SDA regulates the use of these four types of surveillance device differently. For example, it is illegal, subject to a few exceptions, to use a listening device, such as a tape recorder, to record a private conversation in any public place without consent.³ On the other hand, a person may use an optical surveillance device, such as a CCTV system or a camera, to record any activity *outside* a building without consent, but must obtain consent to record a private activity indoors.⁴
- 3.4 Under the Act it is also illegal to use some devices to track a person’s movements without their consent. Only those devices *for which the primary purpose is to track* are regulated by the Act.⁵ Other devices that can track, such as mobile phones with GPS capabilities, are not regulated.⁶ We discuss the details of these provisions in Chapter 6.
- 3.5 The SDA also prohibits a person from communicating or publishing details of a private conversation or activity without consent,⁷ and it regulates the use of data surveillance devices such as spyware.⁸ Breaches of the Act are punishable by up to two years imprisonment and/or 240 penalty units (currently \$28 036.80).⁹
- 3.6 Law enforcement officers must apply to a Supreme Court judge or magistrate¹⁰ for a warrant to covertly install and use a surveillance device.¹¹ The Act also allows senior police officers to issue emergency authorisations in some exceptional circumstances to engage in surveillance activities that would otherwise be unlawful.¹² It appears that this procedure is rarely used.¹³ It is an offence to use, communicate or publish the information collected by a surveillance device in these circumstances, except for law enforcement purposes.¹⁴
- 3.7 Each law enforcement agency must keep detailed records of the types of devices used, the people involved in executing the warrant, and submit a report to the judge or magistrate who issued the warrant. The agency must also submit an annual report to the Minister that includes the number of applications for warrants and the number of ensuing arrests and prosecutions.¹⁵

- 3.8 The Special Investigations Monitor (SIM) is a statutory agency with a range of monitoring functions concerning bodies that deal with police corruption and organised crime. It also has an oversight role in relation to police use of surveillance devices under the Act. The SIM must inspect the records of law enforcement agencies to determine compliance with the Act and report to parliament and to the Minister on its findings.¹⁶ The SIM is entitled to access documents and to request information from agency staff members about an investigation.¹⁷
- 3.9 The SDA does not apply to the Australian Federal Police and other Commonwealth agencies,¹⁸ which are regulated by the *Surveillance Devices Act 2004* (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.¹⁹ In addition, there are a number of other Commonwealth laws that authorise the use of surveillance for law enforcement purposes and for the protection of national security.²⁰ These are discussed in detail in our Consultation Paper.

INFORMATION PRIVACY LEGISLATION

- 3.10 The *Privacy Act 1988* (Cth) (Privacy Act) and the *Information Privacy Act 2000* (Vic) (IPA) regulate the handling of 'personal information'²¹ by government agencies and large private organisations.²² The Privacy Act contains principles that cover the operations of Commonwealth government agencies²³ and slightly different principles that apply to large private sector organisations.²⁴ The IPA has a set of principles that cover Victorian government agencies.²⁵ These are modelled on the Commonwealth principles for large organisations.
- 3.11 All three sets of privacy principles deal with the collection, accuracy, security, use and disclosure of personal information. They also stipulate that collectors of personal information must set out their practices in a public document and provide access and collection rights. In addition, the principles covering large organisations and Victorian agencies have provisions relating to the creation of unique identifiers, anonymity and pseudonymity, restrictions on transborder dataflows, and 'sensitive' personal information.

- 1 *Privacy Act 1988* (Cth), *Information Privacy Act 2000* (Vic).
- 2 Victoria, Parliamentary Debates, Legislative Assembly, 25 March 1999, 192 (Jan Wade).
- 3 *Surveillance Devices Act 1999* (Vic) s 6.
- 4 *Surveillance Devices Act 1999* (Vic) ss 3, 7.
- 5 *Surveillance Devices Act 1999* (Vic) s 8.
- 6 See definition of 'tracking device': *Surveillance Devices Act 1999* (Vic) s 3.
- 7 *Surveillance Devices Act 1999* (Vic) s 11.
- 8 *Surveillance Devices Act 1999* (Vic) s 12. This type of surveillance is not within the scope of this reference. See Chapter 1.
- 9 *Surveillance Devices Act 1999* (Vic) ss 6, 7, 8. Under these sections, a corporation is liable to a maximum penalty of 1200 penalty units (currently \$140,184). This amount is current until 30 June 2010.
- 10 An application can be made to a Supreme Court judge in relation to any surveillance device, and to a magistrate in relation to the use of a tracking device only: *Surveillance Devices Act 1999* (Vic) s 15(3).
- 11 *Surveillance Devices Act 1999* (Vic) Pt 4.
- 12 *Surveillance Devices Act 1999* (Vic) Pt 4 div 3.
- 13 Consultations 16, 25.
- 14 *Surveillance Devices Act 1999* (Vic) ss 30E, 30F.
- 15 *Surveillance Devices Act 1999* (Vic) ss 30M, 30K, 30L.
- 16 *Surveillance Devices Act 1999* (Vic) ss 30P(1), 30Q.
- 17 *Surveillance Devices Act 1999* (Vic) s 30P(2).
- 18 *Surveillance Devices Act 1999* (Vic) s 5.
- 19 See definition of 'relevant offence': *Surveillance Devices Act 2004* (Cth) s 6.
- 20 See *Telecommunications (Interception and Access) Act 1979* (Cth); *Australian Security Intelligence Organisation Act 1979* (Cth); *Aviation Transport Security Act 2004* (Cth); *Crimes Act 1914* (Cth).
- 21 Personal information is defined as being information or an opinion (including information or an opinion forming part of a database), 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. See *Privacy Act 1988* (Cth) s 6 (read in conjunction with section 16B); *Information Privacy Act 2000* (Vic) s 3.
- 22 Small businesses—those with an annual turnover of less than \$3 million—are exempt from the laws: *Privacy Act 1988* (Cth) s 6D(1)–(2).
- 23 *Privacy Act 1988* (Cth) div 3.
- 24 *Privacy Act 1988* (Cth) s 13A, sch 3.
- 25 *Information Privacy Act 2000* (Vic), sch 1. 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.

- 3.12 In its 2008 report, *For Your Information: Australian Privacy Law and Practice*, the ALRC noted that 'Australian privacy laws are multi-layered, fragmented and inconsistent'.²⁶ The ALRC recommended the creation of a unified set of privacy principles to apply to all federal government agencies and the private sector,²⁷ and to state and territory government agencies through an intergovernmental cooperative scheme.²⁸ In its response in October 2009 the Commonwealth Government committed to enacting a single set of Privacy Principles, noting that this 'will mark a significant step toward consistent privacy laws in Australia'.²⁹ The government noted that the ultimate aim was to have a 'consistent set of privacy standards for the Commonwealth, state and territory public sectors, as well as the private sector' and that additional national consistency issues would be considered in the government's second stage response.³⁰

INFORMATION PRIVACY LAWS AND PUBLIC PLACE SURVEILLANCE

- 3.13 Although information privacy laws regulate some types of public place surveillance³¹ there are a number of reasons why many of the more common public place surveillance activities fall beyond the reach of these laws. First, information privacy laws do not apply to all members of the community; they apply only to government agencies and businesses with a gross annual turnover of more than \$3 million. Individuals and smaller businesses are not covered.³² In 2008 the ALRC recommended the removal of the small business exemption in the Privacy Act.³³ The government will consider this recommendation in its second stage response to the ALRC report.³⁴
- 3.14 Secondly, as information privacy laws cover only information that is recorded, they do not apply to any surveillance activities that do not involve the recording of information.³⁵
- 3.15 Thirdly, information privacy laws apply only to 'personal information'; that is, information collected about an individual 'whose identity is apparent, or can reasonably be ascertained, from the information or opinion'.³⁶ The extent to which surveillance-captured information falls within this description is not clear. The Victorian Civil and Administrative Tribunal (VCAT) has found a surveillance-captured image to be 'personal information' in cases where the image was directly linked to other information about an individual.³⁷ This may occur when someone who knew the individual held the image, or when the image was accompanied by the individual's name. Thus, a CCTV-recorded image of a person may be 'personal information' if, for example, that person's image is also on the organisation's security blacklist.
- 3.16 The limited case law does not provide much guidance about the circumstances in which a person's identity 'can be reasonably ascertained'. In one case it was decided that this may extend to circumstances in which it is possible for an organisation to cross-match information within its own databases, but not necessarily with an external database to which it has access.³⁸ Therefore, if someone's identity can be ascertained by reference to external material that may be obtained without an obscure or lengthy process, the information may be 'personal information' covered by Commonwealth and state privacy laws.³⁹
- 3.17 Although some surveillance-captured information is about identified individuals, it is unlikely that the majority of images captured on a public place CCTV system constitute 'personal information' for the purposes of information privacy laws. This is because the identity of many of the individuals depicted cannot be 'reasonably ascertained' from the footage.

3.18 The ALRC has recommended clarifying the scope of the definition of ‘personal information’ by narrowing it, saying:

*a great deal of information is about potentially identifiable individuals but where identifying the individuals would involve unreasonable expense or difficulty, and is unlikely to happen, the ALRC is of the view that the information is not ‘personal information’ for the purposes of the Privacy Act.*⁴⁰

3.19 The ALRC recommended that the definition of personal information should be amended to be information about an ‘identified or reasonably identifiable individual’ (emphasis added).⁴¹ This would bring it in line with international standards and precedents.⁴² The government has accepted this recommendation.⁴³

3.20 The Commonwealth government also accepted the ALRC’s recommendation that the definition of ‘sensitive information’ (a kind of personal information given extra protection under privacy laws)⁴⁴ be changed so that it unequivocally includes biometric information.⁴⁵ Therefore, in the future, organisations that capture biometric information through public place surveillance will have to comply with information privacy laws if this legislation is enacted.

3.21 The commission is of the view that the extent to which surveillance-captured information is governed by information privacy law requires clarification. The Commonwealth Government accepted the ALRC’s recommendation that the Federal Privacy Commissioner develop and publish guidance on the meaning of ‘identified or reasonably identifiable individual’.⁴⁶ The Victorian Privacy Commissioner should be encouraged to liaise with the Federal Privacy Commissioner in order to ensure a consistent response to this complex issue.

ENFORCEMENT OF INFORMATION PRIVACY LAWS

3.22 The Federal and Victorian Privacy Commissioners have the power to receive complaints about bodies that may have contravened information privacy laws.⁴⁷ The Federal Privacy Commissioner received 1089 new complaints in 2008–9.⁴⁸ The Victorian Privacy Commissioner received 88 new complaints in 2008–9.⁴⁹

26 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008) [3.1].

27 *Ibid* 110–111.

28 *Ibid* 25, rec 3–4.

29 Australian Government, *Australian Government First Stage Response to the Australian Law Reform Commission Report 108: For Your Information: Australian Privacy Law and Practice* (2009) 13.

30 *Ibid* 13.

31 See *WL v La Trobe University* [2005] VCAT 2592; *Smith v Victoria Police* [2005] VCAT 654; *Ng v Department of Education* [2005] VCAT 1054; *Re Pasla and Australian Postal Corporation* (1990) 20 ALD 407; *Kiernan v Commissioner of Police, NSW Police* [2007] NSWADT 207. See also 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.

32 *Privacy Act 1988* (Cth) ss 6(1), 7; *Information Privacy Act 2000* (Vic) ss 9, 17(2).

33 Australian Law Reform Commission, above n 26, rec 39–1.

34 Australian Government, above n 29, 14.

35 *Privacy Act 1988* (Cth) s 16B; *Information Privacy Act 2000* (Vic) s 3.

36 *Privacy Act 1988* (Cth) s 6(1); *Information Privacy Act 2000* (Vic) s 3.

37 See *Smith v Victoria Police* [2005] VCAT 654; *Ng v Department of Education* [2005] VCAT 1054; *Re Pasla and Australian Postal Corporation* (1990) 20 ALD 407; *Kiernan v Commissioner of Police, NSW Police* [2007] NSWADT 207.

38 *WL v La Trobe University* [2005] VCAT 2592.

39 Christa Ludlow, ‘“The Gentlest of Predations”: Photography and Privacy Law’ (2006) 10 *Law Text Culture* 135, 145–6 discussing *Police Force of Western Australia v Ayton* [1999] WASCA 233.

40 Australian Law Reform Commission, above n 26 [6.57].

41 *Ibid* rec 6.1.

42 Including the APEC Privacy Framework, the OECD Guidelines, the Council of Europe Convention and the EU Directive; Australian Law Reform Commission, above n 26 [6.53].

43 Australian Government, above n 29, 24.

44 *Privacy Act 1988* (Cth) sch 3; *Information Privacy Act 2000* (Vic) sch 1.

45 Australian Government, above n 29, 25.

46 *Ibid* 24.

47 *Privacy Act 1988* (Cth) s 36(1); *Information Privacy Act 2000* (Vic) s 25(1).

48 Office of the Federal Privacy Commissioner, *The Operation of the Privacy Act Annual Report 1 July 2008–30 June 2009* (2009), 6, 54.

49 Office of the Victorian Privacy Commissioner, *Annual Report 2008–9* (2009) 22–3.

- 3.23 The Federal Privacy Commissioner can investigate a complaint, including by way of obtaining information and documents and examining witnesses.⁵⁰ The Commissioner can make a non-binding order for the payment of damages and institute court proceedings to enforce a determination.⁵¹ The government recently accepted the ALRC's recommendation that the Commissioner should be granted additional powers, including the power to seek civil penalties for serious or repeated breaches of the Privacy Act.⁵²
- 3.24 The Victorian Privacy Commissioner can investigate and conciliate a complaint.⁵³ Conciliation may involve an undertaking by one of the parties to take some action, including the provision of compensation or an apology.⁵⁴ The Commissioner can serve a compliance notice when there has been a 'serious or flagrant contravention' of the IPA or an organisation has committed a breach of the Act at least five times within the previous two years.⁵⁵ It is an offence not to comply with a compliance notice.⁵⁶ To date the Commissioner has issued two compliance notices.⁵⁷
- 3.25 If conciliation fails, the Victorian Privacy Commissioner may refer a complaint to VCAT at the request of the complainant.⁵⁸ The Minister may also refer a complaint directly to VCAT if he or she considers that the complaint 'raises an issue of important public policy'.⁵⁹ When VCAT finds that a complaint is legitimate, it may make a number of orders. These include restraining the respondent from repeating or continuing the act or payment of compensatory damages up to \$100,000.⁶⁰

REGULATION OF SPECIFIC ASPECTS OF PUBLIC PLACE SURVEILLANCE

- 3.26 Some of the most offensive forms of surveillance and behaviours accompanying surveillance are separate criminal offences. There are, for example, Victorian and Commonwealth laws dealing with child pornography,⁶¹ stalking⁶² and harassment (including by the use and dissemination of an image).⁶³ Since 2007 there has also been a law that prohibits 'upskirting'.⁶⁴
- 3.27 There are also some laws that regulate the use of surveillance by specific industries and organisations. The *Private Security Act 2004 (Vic)* imposes a competency requirement on private investigators and private security officers that includes completing approved training.⁶⁵ Training can comprise knowledge of the law relevant to surveillance, including the storage and protection of information gathered.⁶⁶
- 3.28 The *Casino Control Act 1991 (Vic)* has specific laws governing the installation and operation of security cameras. The Act requires clubs to develop procedures for their use,⁶⁷ and establishes the Victorian Commission for Gambling Regulation as the oversight body for the operation of security cameras in gaming clubs.⁶⁸ The *Liquor Control Reform Act 1998 (Vic)* provides that installation of security cameras may be a condition of a liquor licence. There may also be conditions about the quality of images and modes of operation.⁶⁹
- 3.29 There are also laws that make it illegal to drive a taxi not fitted with a functioning camera and to interfere with such a camera.⁷⁰ It is also illegal to download, print or disclose any images or other data from a taxi camera without authorisation.⁷¹

COMMON LAW PROTECTIONS

- 3.30 As well as the laws made by Commonwealth, state and territory parliaments, Australia has a system of common law that is developed through decisions of the courts. The common law regulates some surveillance activities, but does so indirectly when protecting other interests, such as those in property.
- 3.31 In some instances a person can take action for trespass or nuisance to protect their privacy if surveillance activities interfere with their interest in land.⁷² A person may, for example, bring a trespass action to prevent other people from entering his or her land to engage in surveillance activities. A person may also bring a nuisance action to prevent someone from persistently conducting video surveillance of his or her property.⁷³ Importantly, the actions of trespass and nuisance provide limited protection in relation to public place surveillance because only owners of private land can bring these actions before a court.
- 3.32 Although two Australian trial courts have recognised a right to sue for an invasion of privacy,⁷⁴ there are no decisions of the Australian High Court or intermediate appellate courts that have confirmed the existence of this right. This issue is discussed in detail in Chapter 7.

THE VICTORIAN CHARTER OF HUMAN RIGHTS AND RESPONSIBILITIES

- 3.33 The *Charter of Human Rights and Responsibilities Act 2006* (Vic) (the Charter) makes it unlawful for public authorities⁷⁵ to act in a way that is incompatible with the human rights contained in the Charter.⁷⁶
- 3.34 The Charter right of most relevance to public place surveillance is the right to privacy in section 13—the right for a person ‘not to have his or her privacy, family, home or correspondence unlawfully or arbitrarily interfered with’.⁷⁷ This section is modelled on a similar provision in the *International Covenant on Civil and Political Rights* (ICCPR)—a treaty to which Australia is a party.⁷⁸ Section 12 of the Charter, which refers to the right to freedom of movement, is also relevant.⁷⁹

- 50 *Privacy Act 1988* (Cth) ss 40, 44, 45.
- 51 *Privacy Act 1988* (Cth) ss 52(1)(B)(iii), 55A.
- 52 Australian Government, above n 29, 12.
- 53 *Information Privacy Act 2000* (Vic) s 34. The Commissioner also has the power to decline, dismiss, refer or conciliate the complaint in certain circumstances. See *Information Privacy Act 2000* (Vic) ss 29, 30, 33, 34A.
- 54 See eg, *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.
- 55 *Information Privacy Act 2000* (Vic) s 44(1).
- 56 In the case of a body corporate the offence attracts 3000 penalty units; in any other case 600 penalty units: *Information Privacy Act 2000* (Vic) s 48.
- 57 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.
- 58 *Information Privacy Act 2000* (Vic) s 37.
- 59 *Information Privacy Act 2000* (Vic) s 31(1).
- 60 *Information Privacy Act 2000* (Vic) ss 43(1) (a).
- 61 *Crimes Act 1958* (Vic) ss 68–70; *Criminal Code Act 1995* (Cth) sch [474.19].
- 62 *Crimes Act 1958* (Vic) s 21A.
- 63 *Criminal Code Act 1995* (Cth) sch [474.17].
- 64 *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.
- 65 *Private Security Act 2004* (Vic) ss 25(3), 182.
- 66 See Australian School of Security and Investigations, *Certificate III in Investigative Services* (2009) <www.trainingschool.com.au/certificate3.html> at 26 October 2009.
- 67 *Casino Control Act 1991* (Vic) s 122(1)(r).
- 68 *Casino Control Act 1991* (Vic) s 59(2)(b).
- 69 *Liquor Control Reform Act 1998* (Vic) s 18B.
- 70 *Transport (Taxi-Cabs) Regulations 2005* (Vic) regs 15, 22.
- 71 *Transport Act 1983* (Vic) s 158B–C.
- 72 An action for trespass requires showing 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, 529.
- 73 *Raciti v Hughes* (1995) 7 BPR 14837. See also *Stoakes v Brydes* [1958] QWN 5; *Khorasandjian v Bush* [1993] QB 729.
- 74 *Grosse v Purvis* [2003] QDC 151; *Jane Doe v Australian Broadcasting Corporation* [2007] VCC 281.
- 75 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.
- 76 *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 38(1).
- 77 *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 13(a).
- 78 *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171, art 17 (entered into force 23 March 1976).
- 79 Guidelines suggest that surveillance that 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: Guidelines for Legislation and Policy Officers in Victoria* (2008).

- 3.35 There has not been any judicial consideration of the scope of the right to privacy in section 13 of the Charter. However, the United Nations Human Rights Committee (the Human Rights Committee), the body charged with monitoring implementation of the ICCPR, has recognised that the right to privacy may be breached through some surveillance practices.⁸⁰ Likewise, the European Court of Human Rights, in considering the right to privacy under the European Convention on Human Rights, found invasions in relation to publication of photographs of a celebrity⁸¹ and television broadcast of CCTV street footage.⁸²
- 3.36 Draft guidelines prepared by the Victorian Department of Justice (DOJ Draft Guidelines),⁸³ 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.⁸⁴

LIMITS ON THE RIGHT TO PRIVACY UNDER THE CHARTER

- 3.37 The Charter recognises that the right to privacy is not absolute. Section 13 of the Charter prohibits interferences with the right to privacy only if they are unlawful or arbitrary. The term 'arbitrary' has not yet been considered by a court in Victoria. The Human Rights Committee has said that an interference is not arbitrary if it is 'reasonable',⁸⁵ that is, proportionate to the end sought and necessary in the circumstances.⁸⁶
- 3.38 In order to demonstrate that surveillance is reasonable, guidelines prepared by the Department of Justice say that a public authority using surveillance must be able to demonstrate that the limitation on privacy 'is justified in the circumstances'.⁸⁷ The guidelines also suggest that
- the purported purpose of the surveillance must at minimum be a societal concern that is pressing and substantial and this is more than just an effort to achieve a common good⁸⁸ and
 - the purpose of surveillance would need to relate to an area of public or social concern that is important, and not trivial. Economic considerations alone (other than a serious fiscal crisis) will almost never be important enough to justify a limitation to a right.⁸⁹
- 3.39 In addition, any right under the Charter may be limited by the application of another right. For example, although 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.⁹⁰ Section 7(2)—the general limitations clause—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 a number of factors, including the importance of the right to freedom of expression in the particular context.⁹¹ The right to privacy, and other rights potentially affected by public place surveillance, are discussed more in Chapter 4.

NON-BINDING GUIDELINES, STANDARDS AND POLICIES

- 3.40 Because few laws regulate surveillance in public places, users of surveillance generally look to advisory guidelines and industry standards, or devise their own internal policies and procedures, to determine which surveillance practices are permissible and which are unacceptable.

3.41 A number of non-binding guidelines, standards and policies have been developed, particularly covering common forms of surveillance. For example, the Federal and Victorian Privacy Commissioners have written advisory guidelines about the application of privacy law, some of which have relevance to public place surveillance.⁹² The Australian Institute of Criminology also recently developed guidelines for the use of public place CCTV.⁹³ Some government departments and local councils have developed their own internal protocols, particularly for their use of CCTV. These generally include who can access, download and copy footage and how this should be done, as well as how footage should be securely stored.

3.42 Guidelines for compliance with legislation have also been developed at an industry level. For example, the Australian Institute of Petroleum and the Federal Police have developed national guidelines for petrol service station use of surveillance cameras.⁹⁴ In addition, many individual users of surveillance in public places told the commission that they follow internal policies and practices in relation to the collection and storage of footage, and its provision to third parties. Examples of major relevant guidelines, standards and policies are provided in Table 2 on page 57. These are discussed in detail in our Consultation Paper.⁹⁵

REGULATION IN OTHER JURISDICTIONS

OTHER AUSTRALIAN JURISDICTIONS

3.43 All Australian states and territories have legislation that regulates the use of surveillance devices, although some jurisdictions deal only with the use of listening devices.⁹⁶ NSW, the Northern Territory, South Australia and Western Australia all have laws that extend to devices other than listening devices, as in Victoria.⁹⁷ These Acts are similar to the SDA, but there are some important distinctions. These are discussed in Chapter 6.

3.44 Similarly, each Australian state and territory regulates the management of personal information by public authorities through either a legislative regime or an administrative scheme.⁹⁸ The regulation of the handling of personal information in other Australian jurisdictions is discussed in detail in our Consultation Paper.

80 Including telephone tapping and interference with the correspondence of prisoners: Sarah Joseph et al, *The International Covenant on Civil and Political Rights: Cases, Materials and Commentary* (2nd ed) (2004) 492.

81 *Von Hannover v Germany* 59320/00 [2004] VI Eur Court HR 294 [61].

82 *Peck v United Kingdom* 44647/98 [2003] I Eur Court HR 44.

83 Human Rights Unit, Department of Justice [Victoria], above n 79.

84 *Ibid* 81.

85 Human Rights Committee, General Comment 16 (Twenty-third session, 1988). Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, UN Doc HRV/GEN/1/Rev.6 at 142 (2003) [4].

86 *Toonen v Australia*, Human Rights Committee, Communication no 488/1992, UN Doc CCPR/C/50/D/488/1992 (31 March 1994) [8.3].

87 Human Rights Unit, Department of Justice [Victoria], above n 79, 42.

88 *Ibid* 43.

89 *Ibid* 43.

90 '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).

91 Human Rights Unit, Department of Justice [Victoria], above n 79, s 2.2.

92 See eg, Office of the Federal Privacy Commissioner and Human Rights and Equal Opportunity Commission, *Covert Surveillance in Commonwealth Administration: Guidelines* (1992); Office of the Victorian Privacy Commissioner, *Mobile Phones with Cameras* Info Sheet 05.03 (2003).

93 Australian Institute of Criminology, *Considerations for Establishing a Public Space CCTV Network* (2009).

94 Roundtable 20.

95 Victorian Law Reform Commission, *Surveillance in Public Places*, Consultation Paper 7 (2009), 113–6.

96 See *Listening Devices Act 1992* (ACT); *Invasion of Privacy Act 1971* (Qld); *Listening Devices Act 1991* (Tas).

97 *Surveillance Devices Act 2007* (NSW); *Surveillance Devices Act 2007* (NT); *Listening and Surveillance Devices Act 1972* (SA); *Surveillance Devices Act 1998* (WA).

98 *Privacy and Personal Information Protection Act 1998* (NSW); *Australian Capital Territory Government Service (Consequential Provisions) Act 1994* (Cth); *Information Act 2002* (NT); *Information Standard 42—Information Privacy* (IS 42), issued by the Queensland Department of Innovation and Information Economy under the *Financial Management Standard 1997* (Qld); *PC012 – Information Privacy Principles Instruction*, Government of South Australia (1992). The *Information Privacy Bill 2007* (WA) was introduced into the Western Australian Parliament in March 2007. The Bill has not yet passed through both houses of the Western Australian Parliament.

OTHER COUNTRIES

- 3.45 Public place surveillance is more directly regulated in some other countries than it is in Victoria. In the UK,⁹⁹ New Zealand,¹⁰⁰ Canada,¹⁰¹ Ireland,¹⁰² Norway¹⁰³ and the Netherlands¹⁰⁴ surveillance practices are regulated through data protection or privacy laws. In a recent development, the UK Minister for Policing announced the creation of a new National CCTV Oversight Body and appointed an interim CCTV regulator. The regulator will work with the National CCTV Strategy Board to develop recommendations about the use of CCTV in public places.¹⁰⁵
- 3.46 Other countries, such as Sweden,¹⁰⁶ Denmark,¹⁰⁷ and France,¹⁰⁸ have separate laws that specifically regulate surveillance in public places. In addition, some countries have created a right to sue for invasion of privacy, either through the courts or by legislation. These models are discussed in Chapter 7.

CONCLUSION

- 3.47 Although 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. Devices have become increasingly affordable, available and sophisticated. The two major bodies of law regulating public place surveillance—the SDA and information privacy laws—are limited when it comes to public place surveillance because they were not specifically designed to regulate this activity.
- 3.48 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. Victorians 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.

TABLE 1: LEGISLATION AND BINDING CODES RELATING TO PUBLIC PLACE SURVEILLANCE IN VICTORIA

LEGISLATION	APPLICATION TO PUBLIC PLACE SURVEILLANCE	USERS COVERED
<i>Privacy Act 1988</i> (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
<i>Surveillance Devices Act 2004</i> (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
<i>Telecommunications (Interception and Access) Act 1979</i> (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
<i>Casino Control Act 1991</i> (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
<i>Charter of Human Rights and Responsibilities Act 2006</i> (Vic), in particular 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.	Victorian Government agencies and contracted service providers
<i>Crimes Act 1958</i> (Vic) s 68	Prohibits the production of child pornography.	All
<i>Crimes Act 1958</i> (Vic) s 21A	Prohibits stalking.	All

- 99 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.
- 100 Privacy Commissioner [New Zealand], *Privacy and CCTV: A guide to the Privacy Act for businesses, agencies and organisations* (2009) <www.privacy.org.nz/privacy-and-cctv-a-guide-to-the-privacy-act-for-businesses-agencies-and-organisations> at 26 October 2009.
- 101 *Privacy Act* RS C 1985 c P-21; *Personal Information Protection and Electronic Documents Act* RS C 2000 c 5.
- 102 See Office of the Data Protection Commissioner, Ireland, *What Issues Surround the Use of CCTV?* <www.dataprotection.ie/viewdoc.aspx?DocID=642> at 19 January 2009.
- 103 Act of 14 April 2000, No 31 relating to the processing of personal data (Personal Data Act) (Norway).
- 104 College Bescherming Persoonsgegevens, *If You Record People on Video Camera Fact Sheets* 20A (2005), 20B (2005).
- 105 *Briefing 15.12.09: National CCTV Oversight Body*, The National CCTV Strategy Board, Home Office <www.crimereduction.homeoffice.gov.uk/cctv/cctv_oversight_body_b.pdf> at 20 January 2010.
- 106 Electronic Privacy Information Center and Privacy International, *Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments* (2007).
- 107 *Ibid* 402.
- 108 Marianne Gras, 'The Legal Regulation of CCTV in Europe' (2004) 2 *Surveillance & Society* 216, 222-3.

3

Chapter 3

Current Law



LEGISLATION	APPLICATION TO PUBLIC PLACE SURVEILLANCE	USERS COVERED
<i>Information Privacy Act 2000</i> (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
<i>Health Records Act 2001</i> (Vic)	Regulates the handling of health information. Contains a set of Health Privacy Principles (HPPs) based on the NPPs.	Victorian Government agencies and private health service providers
<i>Surveillance Devices Act 1999</i> (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
<i>Liquor Control Reform Act 1998</i> (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
<i>Summary Offences Act 1966</i> (Vic) div 4A	Prohibits upskirting.	All
<i>Summary Offences Act 1966</i> (Vic) s 17	Prohibits indecent, offensive, or insulting behaviour in public.	All
<i>Private Security Act 2004</i> (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
<i>Transport (Taxi-Cabs) Regulations 2005</i> (Vic) ss 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
<i>Transport Act 1983</i> (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 cannot be unlawfully installed in a taxi.	Taxi operators and drivers

LEGISLATION	APPLICATION TO PUBLIC PLACE SURVEILLANCE	USERS COVERED
Binding codes	Application to public place surveillance	Users covered
<i>Biometrics Institute Privacy Code</i> (Cth)	Substantially similar to the National Privacy Principles (NPPs) under the <i>Privacy Act 1998</i> (Cth), but tailored to organisations using or planning to use biometrics.	Biometrics Institute members who have agreed to be covered by the Code
<i>Market and Social Research Privacy Code</i> (Cth)	Substantially similar to the NPPs, but tailored to the market and social research context.	Association of Market and Social Research Organisations members
Media codes	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

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	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	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



GUIDELINES			
Organisation	Instrument	Application to public place surveillance	Users covered
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 <i>Information Privacy Act 2000</i> (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 station 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
Standards Australia	Australian Standard: Closed circuit television (CCTV), Parts 1–3	Includes 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



Chapter 4
**A Balanced Approach to
Regulation**

CONTENTS

- 60 Introduction
- 60 The impact of public place surveillance
- 60 Benefits
- 64 Risks
- 71 A balanced approach to regulation
- 80 An overview of our recommendations and our approach
- 80 Conclusion

A Balanced Approach to Regulation

INTRODUCTION

- 4.1 In Chapter 2 we described the many ways Victorians experience surveillance in public places. Examples include the widespread presence of CCTV on city streets and in shopping centres, the various surveillance devices in public transport and the increasing use of personal surveillance, such as cameras and GPS in mobile phones.
- 4.2 In this chapter, we consider the impact surveillance is having on the lives of Victorians. In particular, we report what we have learnt from users of public place surveillance, as well as members of the public and community organisations, about the benefits and risks of its use. In response, we have devised a balanced approach to regulation—one that strives to maximise the benefits of public place surveillance while minimising its risks.
- 4.3 In developing our recommendations for reform, the commission has drawn on two particular sources. The first is the *Charter of Human Rights and Responsibilities Act 2006* (Vic) (the Charter). This contains a useful framework for achieving a balanced approach to regulation when rights are in conflict and when there is a need to place limits upon the capacity to exercise a particular right. The second is modern theories of responsible regulation, which are also useful when considering how best to regulate a complex activity where interests may differ quite markedly. We discuss the applicability of these sources to the development of our approach below.
- 4.4 We conclude the chapter by outlining our recommendations for reform in general terms. Chapters 5, 6 and 7 contain detailed discussion of each recommendation.

THE IMPACT OF PUBLIC PLACE SURVEILLANCE

- 4.5 Many questions arise when considering the impact of public place surveillance. Are such activities harmful because they threaten human rights, such as the right to privacy? Will the ‘surveillance society’¹ irreversibly change the way we live because we will always feel we are being watched in public places?
- 4.6 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 of surveillance in public places? David Lyon has noted that we depend on surveillance ‘for the efficiency and convenience of many ordinary transactions and interactions’.³
- 4.7 Characterisation of the risks and benefits of public place surveillance is often challenging because the effects of particular forms of surveillance might be considered beneficial to some people and detrimental to others. Nevertheless, we have prepared an outline of the various benefits and risks as defined in the literature and as explained to us in consultations.

BENEFITS

- 4.8 The uses and users of surveillance have changed markedly over the past few years. Surveillance technology is increasingly able to collect and disseminate information in ways previously not thought possible. Today, police and many other Victorian agencies rely on sophisticated surveillance technology for their everyday operational and business activities. Surveillance devices are also utilised by individuals for a number of important purposes. The commission met a wide variety of users of surveillance, who told us why they use the technology and the benefits they derive from it. These are outlined below.

INVESTIGATION OF CRIMINAL ACTIVITY AND FRAUD

- 4.9 One of the primary benefits of public place surveillance is its use in investigating incidents that may involve criminal behaviour. Victoria Police told the commission that surveillance is an important part of criminal investigations and a key factor in obtaining convictions.⁴ The reasons for police use of surveillance include:
- to obtain evidence of criminal activity
 - to enhance the ability to investigate corruption offences and other forms of crime that are covert, sophisticated and difficult to detect by conventional methods
 - to encourage more defendants to plead guilty to charges because of surveillance evidence
 - to reduce the potential for harm to police, undercover operatives and informants because they can be forewarned of planned reprisals and criminal activities.⁵
- 4.10 In addition to their own surveillance records, police use CCTV footage provided by others, either voluntarily or upon request.⁶
- 4.11 Police also use listening and tracking devices to aid in investigations. For example, the commission was told that some police officers record conversations between themselves and members of the public for evidentiary purposes.⁷ Potential suspects may also be tracked through their mobile phone⁸ or through the use of ANPR.⁹
- 4.12 Insurance companies and private investigators also use various surveillance technologies, including visual surveillance and listening devices, to determine the validity of insurance claims.¹⁰

ASSET PROTECTION AND DETERRENCE OF CRIME

- 4.13 A number of businesses with whom the commission consulted stated that their main reason for installing CCTV was to protect their property.¹¹ Some also said that the visible presence of cameras reduced crime, particularly property crime, such as graffiti, theft and vandalism.¹² We were told that the installation of CCTV cameras in petrol stations, for example, has reduced the number of drive offs from those stations.¹³ Transport operators also suggested that cameras might serve as a general deterrent to crime and other antisocial behaviour on trains, trams and buses.¹⁴ In addition, local councils told the commission that they used surveillance cameras in the hope they would prevent a range of behaviours, including assault, vandalism, drug dealing, street-car racing, and drunk and disorderly behaviour.¹⁵
- 4.14 CCTV footage is used in a number of ways. Shopping centres noted that it assists security staff to identify people who have previously committed crimes and prevent them from offending again.¹⁶ A council employee told us that operators are able to view footage in real time and notify police of criminal activity quickly, which allows them to respond promptly and avoid the situation escalating.¹⁷
- 4.15 Cameras may be combined with other technology or software to assist in the detection of crime. VicRoads, for example, uses fixed and mobile cameras with ANPR technology to automatically detect traffic offences, such as speeding and traffic light offences.¹⁸

- 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 Roundtable 5. Youth groups also noted that police use surveillance footage to draw out confessions: Roundtable 16.
- 5 Consultations 19, 20; Roundtables 5, 16, 30.
- 6 Consultations 19, 20 and Site Visits 5, 11, 13, 14, 15 indicated they had been approached by police for footage.
- 7 Consultation 20.
- 8 Police must obtain a warrant from a magistrate before undertaking this form of surveillance. *Surveillance Devices Act 1999* (Vic) s 8.
- 9 See Victoria Police, *Inquiry into Automatic Number Plate Recognition Technology* (2008) <www.parliament.qld.gov.au/view/historical/documents/committees/TSAFE/inquiry/ANPR%20technology/Submissions/14.pdf> at 14 January 2010.
- 10 Consultation 3.
- 11 See Site Visits 3, 5, 15, 16, 18.
- 12 See eg, Submission 4; Consultations 1, 27; Site Visit 15.
- 13 Roundtable 15.
- 14 Roundtables 3, 4.
- 15 Roundtables 6, 7, 8.
- 16 Submission 25.
- 17 Consultation 27.
- 18 Site Visit 1.

A Balanced Approach to Regulation

- 4.16 Other technologies are also used to detect or prevent crime. For example, RFID technology is widely used in the retail sector to deter and apprehend shoplifters. Stock is fitted with a passive device that sounds an alarm if it passes through a reader (generally at the exit of a store).¹⁹ RFID chips also are used in modern Australian passports to assist in the prevention of identity fraud.²⁰ Other sophisticated technology, such as facial recognition technology, body scanners and residue scanners are also used in some international airports for the same purposes. This is discussed in Chapter 2.
- 4.17 Although crime prevention and control are major reasons for using CCTV, the evidence suggests its effectiveness in reducing crime is debateable. This is discussed below.

SAFETY

- 4.18 Another important benefit of public place surveillance is the promotion of community and employee safety. The commission was told that CCTV cameras are frequently installed to enhance the safety of an area (including suburban train stations, car parks and some metropolitan streets), particularly at night.²¹ Businesses also use surveillance to protect their employees, particularly those vulnerable to armed robbery, such as petrol stations and bottle shops.²²
- 4.19 Public safety is an important reason underlying the use of surveillance in the transport sector. Surveillance cameras can assist transport operators to respond when a fire has erupted²³ and when determining if passengers are clear of a departing train or tram before allowing it to leave.²⁴ There are over 600 CCTV cameras operated by roads authorities for the purpose of traffic monitoring and accident response.²⁵ Safety is also a major reason for use of surveillance by local councils. Surveillance is used for monitoring road traffic, the movement of fires, access for emergency vehicles and crowd flow at major venues.²⁶
- 4.20 Individuals may also carry surveillance devices to protect themselves and other family members. We were told, for example, of the use of surveillance in domestic violence and family law matters, such as a woman recording her ex-husband's conversations with her as evidence of him breaching his intervention order.²⁷ We were also told of individuals recording scenes at protests 'where there are community concerns that violence may occur'.²⁸ Interestingly, when we consulted community groups—such as youth, multicultural groups and people experiencing homelessness—there was a mixed response to whether CCTV made them feel safer.²⁹
- 4.21 Another way surveillance devices are used to enhance safety is by assisting in locating people who have gone missing. Tracking devices in mobile phones, for example, are used by some parents to keep track of a child's whereabouts,³⁰ and by carers for tracking people suffering from memory loss,³¹ or who have fallen unconscious.³²
- 4.22 Another beneficial use of surveillance devices is in the management of serious incidents or emergencies. For example, in an emergency evacuation camera surveillance can be used to ensure that every person has safely and successfully left the premises.³³ Transport providers and shopping centres told us that camera surveillance has also been useful in facilitating speedy assistance to people if they are injured or in danger.³⁴

OPERATIONAL NEEDS

- 4.23 In addition to its use in the protection of property and promotion of safety, public place surveillance can aid organisations in the everyday operations of their business. For example, cameras and tracking devices are used within the transport sector to monitor traffic flow.³⁵ Recorded footage may also be viewed later to review major incidents or the success of traffic management plans.³⁶ In addition, ANPR and RFID allow speedy billing processes on the road, rail and tram networks.³⁷
- 4.24 RFID tracking is used within many stock supply chains as a method for stock control and distribution.³⁸ Local councils use Google Earth and other satellite technologies to monitor activities, such as illegal housing developments or tree clearing, within their municipality.³⁹
- 4.25 Some organisations use surveillance technologies for advertising or marketing purposes, for example, through mobile phones with Bluetooth functionality.⁴⁰ This is discussed in Chapter 2.

MANAGING THE MOVEMENT AND CONDUCT OF PEOPLE

- 4.26 Surveillance cameras are also used to ensure that public spaces remain accident free by monitoring crowd behaviour. Large stores and entertainment venues use surveillance for public safety purposes and for crowd control. Cameras are monitored and information is passed on to ground staff about how best to manage crowd movement.⁴¹ Surveillance also offers similar benefits for managing the movement of large volumes of people through public transport hubs during busy periods.⁴² Police can access existing CCTV networks (such as those operated by local councils or transport operators) during special events to monitor and manage crowd movement.⁴³

NEWS GATHERING AND THE DISSEMINATION OF INFORMATION

- 4.27 Public place surveillance is a tool used by journalists to record people's activities in public places as part of the newsgathering process. One media organisation told us their activities frequently included 'crowd shots taken at sporting events, filming people participating in street demonstrations, recording of public events and activities, such as outdoor concerts, and recording of events having a public interest dimension, such as police actions'.⁴⁴
- 4.28 The dissemination of information by the media is of great benefit to the public because it allows the community to know about issues as they arise.

ARTISTIC PURPOSES, ENTERTAINMENT AND OTHER PERSONAL USES

- 4.29 Individuals also conduct public place surveillance for a number of beneficial reasons. The use of optical surveillance, such as cameras and video recorders, is commonplace. In its submission to the commission, the Victorian Association of Photographic Societies noted the frequent use of photography by professional and recreational photographers for legitimate artistic purposes to record events and capture images.⁴⁵ People also use audio recording devices—including recorders contained in mobile phones or hand-held computers—to record lectures, presentations or important conversations. Individuals may also use tracking devices in public places for personal purposes. Use of GPS technology in mobile phones and vehicles is now widespread.

- 19 Clive Norris and Gary Armstrong, *The Maximum Surveillance Society: the Rise of CCTV* (1999) 18.
- 20 *The Australian ePassport* (2009) Department of Foreign Affairs and Trade <www.dfat.gov.au/dept/passports/> at 28 January 2010.
- 21 Consultation 22; Site Visits 3, 4, 5.
- 22 Roundtable 15.
- 23 Roundtable 23.
- 24 Site Visit 4.
- 25 Site Visit 1.
- 26 Consultation 5; Roundtable 7; Sue Cant, 'Satellites Help Council Spot Fire Hazards', *The Age* (Melbourne), 16 January 2001, 2.
- 27 Submission 4.
- 28 Submission 34.
- 29 Some people told us that the presence of cameras made them feel safer: Forums 2, 3, 5. Other people said the presence of CCTV cameras did not make them feel safer: Forums 3, 4.
- 30 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.semiossorian.com/story/1158246.html> at 30 June 2008.
- 31 See Katina Michael, Andrew McNamee, M G Michael, 'The Emerging Ethics of Humancentric GPS Tracking and Monitoring' (Paper presented at the International Conference on Mobile Business: IEEE Computer Society, Copenhagen, Denmark, 25–7 July 2006) <ro.uow.edu.au/cgi/viewcontent.cgi?article=1384&context=infopapers> at 21 May 2008.
- 32 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).
- 33 Site Visit 10.
- 34 Submissions 22, 25; Site Visits 2, 4, 15.
- 35 Site Visits 1, 9.
- 36 Site Visit 1; *Think Tram Projects*, VicRoads <www.vicroads.vic.gov.au/Home/PublicTransportAndEnvironment/PublicTransportOnRoads/TramProjects/ThinkTramProjects.htm> at 14 January 2010; *SmartBus Infrastructure*, Department of Transport (Vic) <www.transport.vic.gov.au/web23/Home.nsf/AllDocs/90A14F13EABE24E4CA25766600140C50?OpenDocument> at 28 January 2010.
- 37 Site Visit 1.
- 38 Teresa Scassa et al, 'Consumer Privacy and Radio Frequency Identification Technology' (2005–6) 37 *Ottawa Law Review* 215, 219.
- 39 Lachlan Heywood, 'Public Told not to Fear Council Spies in the Sky', *The Courier Mail* (Brisbane), 19 September 2003, 18.
- 40 *How It Works*, Bluetooth Advertising <www.bluetoothadvertising.com.au/how_it_works.html> at 28 January 2010.
- 41 Site Visits 6, 14; Roundtables 13, 20, 31.
- 42 Site Visits 2, 4.
- 43 Site Visits 1, 5.
- 44 Submission 10.
- 45 Submission 15.

RISKS

- 4.30 Although public place surveillance has many benefits, there are also a number of risks associated with its use. Because some of those risks are subtle and incremental, they may not be widely discussed. Other risks are difficult to characterise. As one privacy commentator has noted, 'most privacy problems lack dead bodies'.⁴⁶ In addition, invasion of privacy may result in harm that the law finds difficult to remedy. We outline below the risks identified by the commission through our research, site visits and consultations.

THREAT TO PRIVACY

- 4.31 Most, if not all, people have reasonable expectations of some privacy in public places. The nature of those reasonable expectations will change according to time and place. Most people would reasonably expect, for example, 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 a busy shopping mall.
- 4.32 Some current surveillance practices may interfere with people's reasonable expectations of privacy in public places. Many people may be shocked to discover that their movements or conversations in public places have been recorded by unseen CCTV cameras or listening devices. The commission was told of numerous instances of surveillance occurring without clear notice to the public.⁴⁷ Even where signs are used, they do not necessarily contain sufficient information: they may not identify why cameras are used; who owns, operates, or is responsible for them; how footage is managed, where it goes, the people to whom it can be released; and how to complain about abuse.⁴⁸
- 4.33 Another surveillance practice that has raised privacy concerns is the use of x-ray body scanners, trialled in 2009, and planned for installation in some Australian airports.⁴⁹ The scanners provide operators with an image of passengers without clothes. A recent UK case of a man caught ogling the image of his colleague has sparked concerns in the UK.⁵⁰
- 4.34 The need to retain privacy in public places is sometimes concerned with the desire to keep particular information private. This information may relate to a person's political views, medical issues (such as attendance at an abortion clinic or a drug and alcohol treatment centre), and social matters (such as attendance at a gay bar).⁵¹ It is strongly arguable that people ought to be able to restrict access to information about themselves of this nature.

SOCIAL EXCLUSION

- 4.35 Young people, Indigenous communities, people experiencing homelessness, and other marginalised and vulnerable members of society use public spaces more than others do because these groups rely on public places as social, living and cultural spaces.⁵² As a result, these groups experience more surveillance in public places than do other members of the community.

4.36 Some submissions pointed out that surveillance in public places has a disproportionate effect on the Indigenous community because of their reliance on public space as cultural space.⁵³ This can lead to individuals feeling targeted. For example, one organisation noted that

*where there is a concentration on policing of street offences, coupled with the increased surveillance of public places, it is understandable that many Aboriginal and Torres Strait Islander People will perceive such actions as aimed directly to their specific use of public space.*⁵⁴

4.37 The St Kilda Legal Service also noted that the presence of surveillance might act to exclude people experiencing homelessness from public places:

*The homeless ... face an increase in the risk of being charged with a range of offences related to their homeless status. For example, if a person is homeless they have far greater likelihood of breaching the law around being intoxicated in a public place. Moreover, if their activities are monitored on CCTV they are more likely to be charged with this offence. The Legal Service is also concerned that increasingly homeless persons are being pushed out of areas where they might previously have found shelter by the proliferation of CCTV cameras. For example, a CCTV camera positioned to record the sheltered waiting area of a railway station may have a 'security' function, but it can also facilitate train authorities 'moving on' a homeless person who uses the area to shelter for the night.*⁵⁵

4.38 Participants in our consultations suggested that CCTV could also exclude other marginalised groups from public places,⁵⁶ For example, including complaints by young people about being moved on when congregating in public areas.⁵⁷

4.39 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. Some community organisations noted that their clients report difficulties arising from the use of surveillance and security in shopping centres.⁵⁸ 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.⁵⁹

Access to services

4.40 Surveillance can also disproportionately affect access to services. The commission was told of a number of instances in which young people and other marginalised groups have been moved on by security guards at shopping complexes and train stations, which has prevented them from enjoying public places and also moved them 'away from sites they have elected to be in because they are safe'.⁶⁰ The commission was informed that security guards frequently use CCTV images to help them identify groups or individuals for attention.⁶¹

4.41 It was suggested that the practice of ejecting 'undesirables' essentially establishes that some people have a less legitimate claim to being in public places than others. The result is that they 'develop a clearer sense of marginalisation and alienation'.⁶² One submission suggested that the right to freedom of movement includes 'the right to avoid being forced to move'.⁶³

46 Solove, above n 2, 768.

47 Eg, Consultation 31; Site Visit 18; Roundtables 5, 25, 26, 27.

48 Roundtable 16.

49 Anthony Albanese MP, Minister for Transport, 'Strengthening Aviation Security' (Press Release, 9 February 2010).

50 Reuters UK (2010), 'Heathrow Worker Warned in Scanner Ogling Claim', <uk.reuters.com/article/idUKTRE62N1TB20100324> at 25 March 2010.

51 Christopher Slobogin, 'Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity' (2002) 72 *Mississippi Law Journal* 213, 244-5.

52 Submissions 12, 20, 32, 40, 42.

53 Submission 20, 40.

54 Submission 20.

55 Submission 14.

56 See eg, Submissions 5, 14, 40, 42.

57 Forums 2, 3, Roundtable 16.

58 Roundtable 18.

59 Walter Siebel and Jan Wehrheim, 'Security and the Urban Public Sphere' (2006) 3 (1) *German Policy Studies* 19, 22.

60 Submission 12. Other submissions expressed similar views, see eg, Submissions 32, 42.

61 Submission 25; Consultation 27; Site Visit 13.

62 Submission 34.

63 Submission 42.



Access to CCTV footage

- 4.42 The issue of access to and retention of surveillance data—in particular CCTV footage—was of concern to several organisations the commission met.⁶⁴ They noted that only those conducting the surveillance are aware of the period of time data are kept, and that community members are unlikely to be able to access the footage in time, particularly if the process involves getting legal advice.⁶⁵ It was suggested that this is indicative of the general power imbalance between users and subjects of surveillance.⁶⁶
- 4.43 We were also told of people who had been victims of assault at nightclubs and other CCTV monitored places who were refused access to the footage of the incident.⁶⁷ In submissions and forums it was alleged that assaults have been committed against members of the public by persons in positions of authority who were aware of the placement of CCTV and intentionally avoided being within its range.⁶⁸ A surveillance user noted that police usually request access to the footage before it has been destroyed but that requests from the public are usually too late.⁶⁹

Inappropriate publication of footage

- 4.44 Another specific concern was with the publication of images captured by surveillance devices of people, particularly children, suspected of having committed criminal offences.⁷⁰ The commission was told that there are CCTV captured images of young people displayed in some shops and shopping complexes.⁷¹ Concern was expressed over the potential impact that this practice can have on young people.⁷² A number of individuals and organisations were of the view that the publishing, dissemination and use of material captured by surveillance also requires regulation.⁷³

LOSS OF ANONYMITY

- 4.45 Some authors have argued that surveillance of public places creates a loss of individual anonymity in public and that this has negative social consequences.⁷⁴
- 4.46 As one commentator noted, ‘under the gaze of CCTV, it is simply impossible to blend into the situational landscape, or to be confident that one is acting anonymously’.⁷⁵ In this way, ‘an ability to spy on the lives of individuals by intrusive methods can not only affect the lives of individuals but can provide a source of power which can have profound effects on wider society’.⁷⁶
- 4.47 Some people expressed concerns about the operation of the new myki public transport card which requires anyone wanting to travel on a concession fare to disclose personal details, while individuals travelling on a full fare can elect to remain anonymous.⁷⁷ People who qualify for concession fares on public transport necessarily have a lower income and are often heavily reliant on public transport as a mode of transportation, making it difficult for them to opt out of such a scheme. A Liberty Victoria spokesperson has stated that ‘from a privacy perspective the myki card is an unofficial tracking device’ because it will register where and at what time an individual has used their card.⁷⁸ ANPR and RFID technology on private toll roads, which is discussed in Chapter 2, allows the movement of vehicles to be tracked.

THE CHILLING EFFECT

- 4.48 The ‘chilling effect’ is a term used to describe the phenomenon of people changing the way they behave in public, even when alone, because they are aware of the presence of surveillance.⁷⁹ Concerns were raised in several consultations and submissions about the way surveillance can affect an individual’s public behaviour.⁸⁰ It was acknowledged that surveillance could have the effect of ‘normalising behaviour to result in a less diverse and more inhibited society’.⁸¹

4.49 The idea that an anonymous observer can alter individual behaviour is not new. Michel Foucault wrote about this effect of surveillance. He described the gaze of surveillance as central to the exercise of power:

*There is no need for arms, physical violence, material constraints. Just a gaze, a gaze to which each individual under its weight will end by interiorising to the point that he is his own overseer, each individual thus exercising this surveillance over, and against, himself. A superb formula: power exercised continuously and for what turns out to be a minimal cost.*⁸²

4.50 As the use of surveillance cameras becomes more widespread, there is a concern that apprehension about unknown monitoring of activities in public places may alter the way in which people behave. People may no longer feel comfortable to act and communicate with a sense of freedom outside private places. For example, people may be less likely to engage in some activities—such as attending an Alcoholics Anonymous meeting, a psychiatrist’s office, or a sexual health clinic—if they believe they may be under surveillance.⁸³

4.51 In a recent case, the UK Court of Appeal expressed concern about the potential chilling effect of surveillance. In that case the police were not permitted to keep photographs they had taken of a man who had participated in a protest. Lord Collins said he was ‘struck by the chilling effect on the exercise of lawful rights such a deployment would have’.⁸⁴

4.52 The decision not to permit the police to retain the photographs was based largely on Article 8 of the European Convention of Human Rights, which protects the right to private life.⁸⁵ This example is important given the recent allegations that Victoria Police may have been sharing surveillance footage of individual protestors with private organisations.⁸⁶

64 Submissions 1, 12, 34, 42.

65 Submission 34.

66 Submission 34.

67 Submission 12.

68 Submission 34; Forum 4.

69 Consultation 4.

70 Submissions 12, 14.

71 Submissions 12, 14.

72 Submission 14.

73 Submissions 5, 12, 14, 18, 33, 41.

74 See eg, Slobogin, above n 51, 239.

75 Benjamin Gould, ‘Open to All? Regulating Open Street CCTV and the Case for “Symmetrical Surveillance”’ (2006) 25(1) *Criminal Justice Ethics* 3, 6.

76 Roger Toulson, ‘Freedom of Expression and Privacy’ (2007) 41 *Law Teacher* 139, 148.

77 Metlink, *Victorian Fares and Ticketing Manual (myki)* (2009) 43 <www.metlinkmelbourne.com.au/fares-tickets/victorian-fares-and-ticketing-manual-myki/> at 23 November 2009.

78 Georgia King-Siem, quoted in Clay Lucas, ‘Myki Tracking Device Warning’, *The Age* (Melbourne), 19 November 2009 <www.theage.com.au/national/myki-tracking-device-warning-20091118-impl.html> at 19 November 2009.

79 Slobogin, above n 51, 242–3.

80 Submissions 5, 30.

81 Submission 30.

82 Michel Foucault, *Discipline and Punish: The Birth of the Prison* (1975) 155.

83 Slobogin, above n 51, 244–5.

84 *Wood v Commissioner of Police of the Metropolis* [2009] EWCA Civ 414 [92] per Lord Collins.

85 *Wood v Commissioner of Police of the Metropolis* [2009] EWCA Civ 414.

86 See eg, Office of the Victorian Privacy Commissioner, ‘Briefing on the Aquasure Memorandum of Understanding’ (Press Release, 10 December 2009).



CRIMINAL CONDUCT AND OFFENSIVE USES

4.53 As surveillance devices become cheaper, they become increasingly accessible to people who may wish to use them for criminal or offensive conduct. For example, there have been several cases of people using hidden cameras to record under the skirts of unsuspecting women.⁸⁷ This practice is known as ‘upskirting’ and is now a specific criminal offence.⁸⁸ Surveillance in public places is also used to facilitate other crimes. For example, covert surveillance cameras have been installed at ATMs to capture individual PINs for the purpose of stealing from individual accounts. There is also the possibility of blackmail based on recorded images of embarrassing conduct.⁸⁹

Recording criminal behaviour as entertainment

4.54 There has been a disturbing trend of people recording their own criminal conduct. In some cases this has involved activities that are especially cruel and violent. In a widely publicised Victorian example, a group of teenage boys lured a teenage girl to a park in Werribee and forced her to remove some of her clothing and perform oral sex. They then set fire to her hair and urinated on her. The young men responsible filmed the entire incident and produced a DVD that they distributed to a number of people.⁹⁰ In another incident in Geelong, five men set upon two teenage girls, sexually assaulted them and filmed the incident on a mobile phone.⁹¹ In a recent case, a woman filmed her 14-year-old daughter assaulting another girl.⁹² Footage from these types of incidents is commonly distributed among friends. There have also been some examples of footage having been posted on the internet.⁹³

Inappropriate recording of emergencies

4.55 Recently, the media have reported incidents in which individuals have used their mobile phones to film emergencies for the apparent purpose of entertainment. In Queensland, after a runaway vehicle hit a backpacker, ‘dozens’ of bystanders apparently filmed the victim’s final moments on their mobile phones.⁹⁴ Similarly, in NSW, after a traffic accident in which children were killed, bystanders began filming the mother’s pleas for assistance and the accident scene.⁹⁵

PUBLICATION ON THE INTERNET

4.56 Digital technologies have increased the capacity of individuals to capture, transmit and distribute recordings of voices and images quickly and easily. The popularity of the mobile camera phone has meant that the distribution of images can be both immediate and widespread. As noted in some consultations and submissions, the development of this technology has meant that embarrassing (but legal) behaviour is increasingly posted on the internet without the consent of the person who would find it most embarrassing.⁹⁶ For example, videos have been posted online of celebrities intoxicated in public places in Melbourne,⁹⁷ and individuals falling over or injuring themselves.⁹⁸

4.57 In at least one consultation, some participants were of the view that if a person, particularly a celebrity, is in a public place they run the risk of being filmed and should be aware that images of them might be distributed.⁹⁹ Others were of the opinion that the use of embarrassing footage as entertainment without the consent of the potentially humiliated party was unacceptable.

4.58 Widespread concerns have been expressed in the media and by privacy advocates about the implications of Google Street View.¹⁰⁰ For example, the Google camera has occasionally captured individuals who are clearly identifiable and unaware their image would be published on the internet via Street View. Overseas it has captured and published images of women sunbathing and a man entering an adult book store.¹⁰¹

SURVEILLANCE MAY NOT WORK

4.59 During consultations the commission was frequently informed that surveillance equipment does not always achieve the purpose for which it was installed. Most commonly, questions were raised about whether CCTV surveillance actually deters crime. In some submissions and consultations people expressed the view that criminals can relatively easily alter their behaviour to avoid surveillance.¹⁰² For example, criminals are often aware of the presence of cameras and will sometimes try to alter their appearance to avoid detection.¹⁰³

4.60 In considering whether surveillance improves security, one organisation stated:

*By pledging to improve 'security' through increased surveillance, politicians pander to voters' anxiety, without addressing its underlying causes. We suspect that commercial interests—those of surveillance technology producers, as well as those of businesses employing surveillance—are equally significant drivers of the increase in public place surveillance.*¹⁰⁴

Technological limits

4.61 During consultations the commission was often reminded that surveillance technology is fallible. We were told, for example, that CCTV systems had sometimes failed to capture footage of a serious incident or failed to produce footage to a standard where the offender was identifiable. Similarly, biometric evidence, often touted as foolproof, can also provide inaccurate results. For example, a number of organisations told us that facial recognition technology has a tendency to register false positives.¹⁰⁵

- 87 Eg 'Man Charged Over "Upskirting" Photos', *Sydney Morning Herald* (Sydney), 6 September 2009 <www.smh.com.au/national/man-charged-over-upskirting-photos-20090906-fccu.html> at 28 January 2010; Karen Matthews, 'Upskirting Case Delayed', *Geelong Advertiser* (Geelong), 24 September 2009 <www.geelongadvertiser.com.au/article/2009/09/24/106781_news.html> at 28 January 2010
- 88 *Summary Offences Act 1966* (Vic) div 4A.
- 89 Submission 5.
- 90 Mex Cooper, 'Werribee DVD Sex Case: Teens' Attack Sickening, Says Girl's Dad', *Geelong Advertiser* (Geelong), 18 October 2007 <www.geelongadvertiser.com.au/article/2007/10/18/7951_news.html> at 18 November 2009; Greg Roberts, 'Boys Escape Detention Over Assault Film', *The Age* (Melbourne), 5 November 2007 <<http://news.theage.com.au/national/boys-escape-detention-over-assault-film-20071105-18ct.html>> at 18 November 2009.
- 91 'Gang Sex Attack Filmed on Mobile Phone', *The Age* (Melbourne), 17 May 2007 <<http://news.theage.com.au/national/gang-sex-attack-filmed-on-mobile-phone-20070517-db9.html>> at 18 November 2009.
- 92 Adrian Lowe, 'Mother Reportedly Videotaped Daughter Assaulting Disabled Girl', *The Age* (Melbourne), 1 December 2009 <www.theage.com.au/national/mother-urged-daughter-to-bash-intellectually-disabled-girl-20091201-k2eo.html> at 1 February 2010.
- 93 See eg, 'Clip of Mother being Gang-Raped Posted on YouTube', *News.Com.Au*, 5 March 2008 <www.news.com.au/story/0,23599,23322566-2,00.html> at 18 November 2009.
- 94 Peter Michael, 'Police Condemn Ghoulis People Who Filmed Backpacker's Dying Moments', *The Courier-Mail* (Brisbane), 8 January 2010 <www.news.com.au/national/police-condemn-ghoulis-people-who-filmed-backpackers-dying-moments-story-e6frfkvr-1225817200736> at 8 January 2010.
- 95 Gemma Jones and Anna Caldwell, 'Onlookers Film Burning Car as Sisters Lay Dying', *The Courier-Mail* (Brisbane), 30 December 2009 <www.news.com.au/couriermail/story/0,1,26535799-952,00.html> at 8 January 2010.
- 96 Submission 5; Forum 4.
- 97 See eg, 'Andrew O'Keefe's Drunk Night on the Tiles' *Herald Sun* (Melbourne) <www.youtube.com/watch?v=MagTxy1Exwo> at 11 November 2009; 'AFL Footy Show—Brendan Fevola Brownlow Street Talk '09 (24 September, 2009) HQ' <www.youtube.com/watch?v=UDSphOXMgbM> at 11 November 2009.
- 98 'Man Falling Over a YouTube Sensation', *Herald Sun* (Melbourne), 12 January 2010 <www.heraldsun.com.au/lifestyle/the-other-side/man-falling-over-a-youtube-sensation/story-e6frfhk6-1225818535649> at 13 January 2010.
- 99 Consultation 12.
- 100 See eg, Lisa Martin, 'Big Brother in the Backyard—Issues in the News—Google Street View', *The Age* (Melbourne), 6 October 2008 16; Kelly Brown, 'Alarm over Street View', *The Hume Moreland Leader* (Melbourne), 13 August 2008, 7; Sharon Labi, 'Google to Limit its Street View', *Herald Sun* (Melbourne), 20 July 2008, 12.
- 101 Labi, above n 100, 12.
- 102 Submissions 20, 30; Forums 1, 3, 4; Consultations 6, 11; Site Visit 5.
- 103 Forum 1.
- 104 Submission 40.
- 105 Consultations 1, 11; Site Visits 10,13.

A Balanced Approach to Regulation

- 4.62 The use of camera footage in conjunction with expert identification evidence in criminal prosecutions has been questioned because it is not always accurate.¹⁰⁶ Experts in criminal prosecutions use facial mapping techniques to compare the face of the accused with that contained in the camera image of the offender. These techniques are neither standardised nor consistently applied. Critics have suggested that as a result this method of identification risks being ‘unreliable and unfairly prejudicial’.¹⁰⁷

Ineffective in preventing crime

- 4.63 Evidence that CCTV is effective in controlling crime remains largely inconclusive.¹⁰⁸ 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’.¹⁰⁹ Brandon Welsh and David Farrington concluded in 2002 that ‘the best current evidence suggests that CCTV reduces crime to a small degree’.¹¹⁰
- 4.64 In Australia there have been few published evaluations of CCTV.¹¹¹ In 2006, Helene Wells and others published results from their research into CCTV use in Gold Coast public spaces and on the Queensland Rail Citytrain network.¹¹² The authors found an increase in total offences against the person after CCTV was installed, compared to areas without CCTV.¹¹³ They concluded it was likely that CCTV detected violent crime that previously went undetected, but it had not prevented it.¹¹⁴
- 4.65 Even when CCTV has been shown to reduce crime rates, that reduction relates only to certain types of crimes. CCTV has been more successful at reducing property crimes,¹¹⁵ and two studies found that CCTV was effective at reducing vehicle theft from car parks.¹¹⁶ CCTV may be less effective at reducing crime against the person and ‘impulsive’ acts such as alcohol-related crime.¹¹⁷ Wells and others also reported that the evidence of CCTV’s effectiveness at reducing burglary was mixed, and that CCTV may have no impact on shoplifting.¹¹⁸
- 4.66 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.¹¹⁹ Similarly, some people in consultations suggested that one response to CCTV use in Melbourne has been that drug dealing has relocated.¹²⁰ Nevertheless, Wilson and Sutton argue the statistical evidence on the displacement effects of CCTV is largely inconclusive.¹²¹

Misleading perceptions of safety

- 4.67 CCTV may be more effective in creating a perception of safety than preventing crime. We learnt in consultations that some people who experience homelessness in Victoria can derive a sense of safety from the presence of surveillance cameras,¹²² although others do not.¹²³ 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.¹²⁴ At least one study has concluded, however, that CCTV installation may not make people feel safer.¹²⁵ 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 costs and risks associated with the installation of surveillance systems.

CONVERGING DEVICES

- 4.68 Many surveillance devices now have a number of capabilities. This phenomenon is sometimes referred to as 'convergence'. A number of people the commission spoke with expressed concern that the expansion of surveillance capabilities in a single device poses new privacy risks and creates challenges for regulation.¹²⁶
- 4.69 It is possible to use one device to gain a very detailed account of what an individual is doing. Some cameras, for example, now include audio as well as visual recording, and contain software to assist with recognition and tracking.¹²⁷
- 4.70 The potential for unreasonable intrusion into people's lives is also increased by improvements in technology that provide greater precision when monitoring and recording activities. Improvements in image clarity, zoom capacity, sound quality and scanning accuracy are a few examples.

A BALANCED APPROACH TO REGULATION

- 4.71 Any regulation of public place surveillance must strive to balance the many risks and benefits associated with its use. The *Charter of Human Rights and Responsibilities Act 2006* (Vic) (the Charter) contains a useful framework for achieving a balanced approach to regulation when rights are in conflict and when there is a need to place limits upon the capacity to exercise a particular right. Modern theories of responsible regulation are also of use when considering how best to regulate a complex activity where interests may differ quite markedly.

THE VICTORIAN CHARTER OF HUMAN RIGHTS AND RESPONSIBILITIES

- 4.72 Victoria is one of two jurisdictions in Australia with a human rights charter.¹²⁸ Modelled on the *International Covenant on Civil and Political Rights* (ICCPR),¹²⁹ the Charter makes it unlawful for public authorities to act in a way that is incompatible with the human rights listed in the Charter.¹³⁰ The Charter defines the term 'public authority' broadly. It includes police, local councils, and private entities that have functions of a public nature.¹³¹
- 4.73 The Charter also requires that statutes be interpreted in a way that is compatible with human rights whenever possible,¹³² and that statements of compatibility with human rights accompany all Bills introduced into parliament.¹³³

Human rights affected by public place surveillance

- 4.74 The Charter provides a useful framework for devising a balanced approach to regulation of public place surveillance because some forms of surveillance may affect a number of rights in the Charter.
- 4.75 Human rights considerations were at the forefront of many views expressed in submissions and consultations. One submission noted that 'the Charter ensures that human rights language and standards will be relevant to regulation of public place surveillance'.¹³⁴ A number of submissions were especially concerned about ensuring adequate protections for individuals,¹³⁵ while others emphasised that the protection of rights should not be taken too far.¹³⁶

The right to privacy

- 4.76 Section 13 of the Charter grants a person the right 'not to have his or her privacy ... unlawfully or arbitrarily interfered with'.¹³⁷ Government agencies should consider this right before installing surveillance devices and undertaking surveillance activities.¹³⁸

106 See esp., Gary Edmond et al, 'Law's Looking Glass: Expert Identification Evidence Derived from Photographic and Video Images' (2008–2009) 20 *Current Issues in Criminal Justice*, 337.

107 Ibid 350–1.

108 See Dean Wilson and Adam Sutton, *Open-Street CCTV in Australia* (2003) 13–15. They note that studies have produced mixed findings. See also 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); Clive Coleman and Clive Norris, *Introducing Criminology* (2000).

109 Helene Wells et al, *Crime and CCTV in Australia: Understanding the Relationship* (2006) 2.

110 Welsh, above n 108, i.

111 See Wilson, above n 108, 112.

112 Wells, above n 109, 4–5.

113 Ibid 78.

114 Ibid iii.

115 Martin Gill and Angela Spriggs, *Assessing the Impact of CCTV* (2005) 3.

116 Ibid 29–30; Welsh, above n 108, vii, 34–40.

117 Gill, above n 115, vii, 33–40, 118.

118 Wells, above n 109, 2 (see studies cited therein).

119 See Vanessa Goodwin, Crime Prevention and Community Safety Council [Tasmania], *Evaluation of the Devonport CCTV Scheme* (2002) 34.

120 Roundtable 6.

121 Wilson, above n 108, 14.

122 Forum 4; Roundtable 16.

123 Forum 4.

124 Roundtables 2, 5, 7.

125 Gill, above n 115, 60–1.

126 Submission 5; Consultation 5.

127 See Chapter 2.

128 The other is the Australian Capital Territory. See the *Human Rights Act 2004* (ACT).

129 Human Rights Unit, Department of Justice [Victoria], *Charter of Human Rights and Responsibilities: Guidelines for Legislation and Policy Officers in Victoria* (2008) 13 (definition of 'human rights').

130 *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 38(1).

131 *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 4.

132 *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 32(1).

133 *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 28(1).

134 Submission 9.

135 Submissions 5, 9, 12, 14, 18, 20, 29, 30, 32, 34, 35, 36, 40, 42, 43.

136 Submissions 4, 10, 15, 21, 25, 26, 28.

137 *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 13(a).

138 Ibid 81.

A Balanced Approach to Regulation

- 4.77 Privacy is, however, notoriously difficult to define.¹³⁹ It is a fluid concept that has developed over time in response to new technologies and changes in cultures and lifestyles.¹⁴⁰ It concerns a range of ideas, including secrecy, confidentiality, solitude, anonymity, control over information, freedom from surveillance and protection of one's reputation.¹⁴¹ Accordingly, one leading commentator has referred to privacy as 'a concept in disarray'.¹⁴²
- 4.78 Privacy is considered by some to be 'essential for freedom, democracy, psychological well-being, individuality, and creativity'.¹⁴³ Privacy enables individuals to develop a 'better constructed' view of themselves and the world around them.¹⁴⁴ It also gives people the freedom to develop, discuss and criticise society and government 'anonymously ... and without fear of community reprisal'.¹⁴⁵
- 4.79 Some authors suggest that protecting a right to privacy can have negative consequences. It can cloak illegal activities by protecting them from scrutiny and inhibit some security and law enforcement steps. The enforcement of privacy rights can also dilute transparency and accountability by limiting the extent to which private activities and conversations can be monitored.¹⁴⁶ There can often be an inherent tension between the security objectives of government and the privacy rights of individual members of the community.

The right to freedom of movement

- 4.80 Public place surveillance may also affect the right to freedom of movement, contained in section 12 of the Charter. Guidelines prepared by the Victorian Department of Justice suggest that surveillance that 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.¹⁴⁷

The right to freedom of expression

- 4.81 Section 15 of the Charter deals with the right to freedom of expression. It protects the right of individuals to express and share views, ideas and information with others.¹⁴⁸ This right has long been considered central to a well-functioning democracy.¹⁴⁹
- 4.82 In a liberal democratic country such as Australia there is a need for 'a public sphere, in which there can be open deliberation of issues of public policy, and the opportunity of learning from such exchanges'.¹⁵⁰
- 4.83 Freedom of expression is of fundamental importance to media organisations. In fact, the term 'freedom of expression' is sometimes used to mean 'press rights'.¹⁵¹ The media are understandably concerned to maintain their capacity to report freely and their relative freedom to use visual and audio recording devices to capture newsworthy information.¹⁵²
- 4.84 There is, however, another perspective to consider. The use of surveillance devices in public places may affect freedom of expression by limiting what people feel comfortable saying and doing in public either because they know they are under surveillance or because they may believe this to be the case. Recent allegations that police have agreed to share law enforcement data about protestors with private organisations provides a useful example.¹⁵³ Individuals exercising their right to protest may be reluctant to express themselves this way if they are aware of being monitored and having information about them distributed to others.

4.85 In some instances there is an inevitable tension between the right to privacy and the right to freedom of expression.¹⁵⁴ When this occurs a balance must be struck between the media's right to pursue their newsgathering role (which also involves the public's right to receive that news) and the privacy rights of individuals who might be affected by the gathering and publication of that news.¹⁵⁵

The right to not be unlawfully deprived of property

4.86 The commission was frequently told in submissions and consultations that surveillance devices are installed primarily for the purposes of protecting property and deterring crime. Property rights are protected in section 20 of the Charter, which provides that 'a person must not be deprived of his or her property other than in accordance with law'.¹⁵⁶ Although Charter rights do not directly protect business, all property owners have rights at law to protect their property.

4.87 Property rights are a fundamental part of our society. Numerous criminal and civil laws protect those rights and impose sanctions upon individuals who interfere with them.

Freedom from fear

4.88 Although freedom from fear is not specifically referred to in the Charter, it is a value that underpins other rights and is a fundamental freedom in the Universal Declaration of Human Rights.¹⁵⁷ It is rarely raised in modern human rights dialogues, causing Chief Justice Spigelman to suggest that it has become 'the forgotten freedom'.¹⁵⁸

4.89 Freedom from fear can be used as an argument in favour of the use of surveillance in public places. One of the primary reasons for the installation of surveillance devices is to improve safety and security. Participants in some of the commission's forums said that surveillance in public places sometimes made them feel safer because, for example, surveillance might have reduced the likelihood that they would become victims of crime.¹⁵⁹

4.90 Conversely, freedom from fear may also be a reason for regulating the use of surveillance in public places. The use of surveillance can be intimidating and can negatively alter the way some members of the public behave in public places.

The Charter's framework for determining when surveillance is justified

4.91 The Charter provides a useful framework for balancing rights. It does this by declaring that human rights are not absolute and that they may be limited in certain circumstances. The human rights in the Charter are subject to 'specific limitations' that are relevant to a particular human right, as well as to a 'general limitations clause' that is relevant to all of the human rights contained in the Charter.

4.92 There is a specific limitation on the right to privacy in section 13 of the Charter. Interferences with the right to privacy are prohibited only if they are unlawful or arbitrary. An interference that is not arbitrary is one that is 'reasonable';¹⁶⁰ that is, proportionate to the end sought and necessary in the circumstances.¹⁶¹ Section 13 invites the balancing of the right to privacy against other ends, and consideration of whether the means used, in this case surveillance, is in fact necessary to achieve that end.

139 See eg, 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, 12. This was also noted in a number of consultations and submissions, see Submission 20. Note the commission's Consultation Paper provides a detailed literature review of the right to privacy.

140 See eg, Danuta Mendelson, 'Illustory Rights to Confidentiality and Privacy in the 21st Century?' (Professorial address delivered at Deakin University, Melbourne, 26 August 2009) 7; John Gilliom, *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy* (2001) 115–136.

141 Daniel Solove, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087, 1088; Daniel Solove, *Understanding Privacy* (2008) 1.

142 Daniel Solove, 'A Taxonomy of Privacy' (2006) 154 *University of Pennsylvania Law Review*, 477.

143 Solove, *Understanding Privacy*, above n 141, 5.

144 *Ibid* 79.

145 *Ibid* 80.

146 *Ibid* 81–2.

147 Human Rights Unit, Department of Justice [Victoria], above n 129, s 12.

148 Barendt, above n 139, 11, 30–1.

149 Roger Toulson, 'Freedom of Expression and Privacy' (2007) 41 *Law Teacher* 139, 139.

150 Jeremy Shearmur, 'Free Speech, Offence and Religion' (2006) 22 *Policy* 21, 22.

151 See eg, Barendt, above n 139, 11, 16.

152 Submission 10.

153 See Office of the Victorian Privacy Commissioner, 'Briefing on Aquasure Memorandum of Understanding' (Press Release, 10 December 2009).

154 See eg, Barendt, above n 139, 11, 30.

155 See *Shering Chemicals Ltd v Falkman Ltd* [1981] 2 WLR 848, 865 (Lord Denning).

156 *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 20.

157 CJ James Spigelman, 'The Forgotten Freedom: Freedom from Fear' (Paper presented at the Sydney Law School, University of Sydney, 17 November 2009 and at the Australian Academy of Law, Sydney 18 November 2009) 1–3, 6.

158 *Ibid* 4.

159 Forum 2. See also Submissions 4, 25.

160 Human Rights Committee, General Comment 16, (Twenty-third session, 1988), Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, UN Doc HRI/GEN/1/Rev.6 at 142 (2003) [4].

161 *Toonen v Australia*, *Human Rights Committee*, Communication no 488/1992, UN Doc CCPR/C/50/D/488/1992 (31 March 1994) [8.3].

- 4.93 The general limitations clause in section 7 of the Charter requires that rights be ‘balanced against each other and against competing public interests’.¹⁶² It states that the human rights contained in the Charter may be subject to action that limits the right, but only if the action is authorised by law. It also says the limitation must be ‘reasonable’ and ‘demonstrably justified in a free and democratic society based on human dignity, equality and freedom’.¹⁶³ When determining whether a limit is reasonable, the following factors must be taken into account:
- the nature of the right
 - the importance and purpose of the limitation
 - the nature and extent of the limitation
 - the relationship between the limitation and its purpose
 - any less restrictive means reasonably available to achieve the purpose that the limitation seeks to achieve.
- 4.94 Section 7 provides a useful framework when human rights conflict, that is, when protecting one person’s rights limits the rights of another. As previously discussed, although 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. In such cases, section 7 instructs us to consider the importance of the right to freedom of expression in that context (‘the importance and purpose of the limitation’) and whether that right was advanced by interfering with the privacy rights of others (‘the relationship between the limitation and its purpose’).¹⁶⁴
- 4.95 One submission explained the restricted way Charter rights can be limited in relation to the use of surveillance in public places. It stated that the Charter requires proportionality between the surveillance practice and the purpose it seeks to achieve:

*This means that a user of surveillance ought to use the least privacy-intrusive means of achieving the purpose, and excessively intrusive forms of surveillance may only be justifiable when designed to protect individuals from grave physical harm.*¹⁶⁵

The Charter’s framework for evaluating the human rights impact of surveillance regulation

- 4.96 The Charter also helps evaluate whether our recommended reforms would adversely affect the human rights of users of surveillance. As noted above, the Charter requires that statements of compatibility with human rights be prepared for all Bills introduced to parliament.¹⁶⁶ Department of Justice Guidelines for preparing these statements offer a model for testing whether our recommended reforms for public place surveillance regulation affect the rights contained in the Charter.¹⁶⁷
- 4.97 The guidelines suggest that, as a first step, a legislator should ask whether draft laws raise human rights issues. For example, laws seeking some controls on public place surveillance would raise the human rights issues identified in this chapter. The scope of each relevant human right should be considered, followed by an evaluation of whether the draft law limits, restricts or interferes with each right.
- 4.98 Next, a legislator must ask whether the limitations or restrictions are reasonable and demonstrably justified after having considered all of the relevant factors in section 7(2) of the Charter.¹⁶⁸

REGULATORY THEORY

- 4.99 Our interest in a balanced approach to regulation of public place surveillance has led us to consider modern theoretical approaches to regulation. Regulatory theory is useful in this context because a ‘responsive regulatory approach’ takes account of the relationship between regulation and those being regulated and offers a graduated approach to enforcement.
- 4.100 We also discuss compliance-based regulatory theory, which is characterised by enforcement mechanisms that actively encourage compliance with desired behaviour. A subset of compliance-based regulatory theory is principle-based regulation, which forms the cornerstone of the commission’s recommendations.
- 4.101 Finally, we discuss the *Victorian Guide to Regulation*, which encapsulates much of the modern writing in regulatory theory and apply its suggested approach to law reform of public place surveillance.

Responsive regulation

- 4.102 ‘Responsive regulation’—an approach developed by Ian Ayres and John Braithwaite—is one of the most influential developments in regulatory theory over the last two decades.¹⁶⁹ This approach to regulation grew out of frustration at the polarised nature of many regulatory debates. Businesses were seen either as entities that needed punishment when they broke the law, or as responsible corporate citizens who could be persuaded to comply. There was no middle ground.¹⁷⁰
- 4.103 As Braithwaite notes, the threat of punishment alone is an ineffective means of regulating business. Moreover, it has the potential to backfire and make situations worse for those people who may be future victims of the harm in question.¹⁷¹ Responsive regulation, however, relies on persuasion and cooperation in the first instance. ‘Consistent punishment of business non-compliance would be a bad policy ... persuasion is normally the better way to go when there is reason to suspect that cooperation with attempting to secure compliance will be forthcoming.’¹⁷²
- 4.104 Ayres and Braithwaite propose a regulatory pyramid to assist in determining when punishment becomes necessary and when persuasion is more appropriate.¹⁷³



Ayres and Braithwaite: Regulatory Pyramid

- 162 Explanatory Memorandum, Charter of Human Rights and Responsibilities Bill 2006 (Vic) 9.
- 163 *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 7(2).
- 164 Human Rights Unit, Department of Justice [Victoria], above n 129, s 2.2.
- 165 Submission 12.
- 166 *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 28(1).
- 167 Human Rights Unit, Department of Justice [Victoria], above n 129.
- 168 Ibid 47–8.
- 169 Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (1992).
- 170 John Braithwaite, ‘Rewards and Regulation’ (2002) 29 *Journal of Law and Society* 12, 19; see also Robert Baldwin and Julia Black, ‘Really Responsive Regulation’ (Law Society Economy Working Paper No 15/2007, London School of Economics and Political Science, 2007).
- 171 Braithwaite, above n 170, 20.
- 172 Ibid 20.
- 173 Ayres, above n 169, 35, 39.

A Balanced Approach to Regulation

- 4.105 The pyramid model emphasises that most effort should be directed towards initiatives at the base of the pyramid. Escalation to methods further up the pyramid should occur only when efforts to secure compliance through persuasion have failed. This reflects that 'cooperative approaches such as education, persuasion and restorative justice are normally better ... as a first strategy'.¹⁷⁴
- 4.106 Having a specific regulator in place to administer the system in question is important to the success of the model. The model works by providing a regulator with flexibility and a range of tools that focus on cooperative compliance and only revert to coercion if efforts at persuasion fail. Self-regulation, co-regulation and direct regulation all fall within the pyramid.¹⁷⁵
- 4.107 Those subject to regulation are essentially categorised into three different groups. First, at the base of the pyramid, the organisation or individual is presumed to be willing to comply. Secondly, in the centre of the pyramid, it is presumed the organisation or individual is rational but needs incentives to comply. Thirdly, the apex of the pyramid deals with the irrational organisation or individual whose actions require a much heavier sanction.
- 4.108 Responsive regulation acknowledges that 'persuasive and compliance-oriented enforcement methods are more likely to work where they are backed up by the possibility of more severe methods'.¹⁷⁶ Thus, where regulation seeks to promote socially responsible ends, there is a need to focus on persuasive means to encourage responsible, law-abiding behaviour. Ayres and Braithwaite write that when creating obligations involving social responsibility, models work best when the regulator has 'benign big guns'.¹⁷⁷ By this the authors mean that 'persuasion will normally only be more effective than punishment in securing compliance when the persuasion is backed up by punishment'.¹⁷⁸ A culture of cooperation is easier to establish when there are serious consequences for misbehaviour, but when supportive methods are the first means of attempting to promote good behaviour.¹⁷⁹

Compliance-based regulation

- 4.109 Many scholars have considered how best to achieve compliance through persuasion. These studies suggest that 'in practice ... officials have often relied on education, persuasion and cooperation rather than deterrence to persuade business to preventatively comply with regulatory goals'.¹⁸⁰ The body of theory that explains this approach can be described as compliance-based regulatory theory.
- 4.110 Compliance-oriented regulation relies on a range of strategies. First, it aims to secure compliance with regulatory goals through '(a) codes of conduct and self-regulation, (b) voluntary agreements between government and industry, (c) industry standards and internal management systems, and (d) economic instruments and market mechanisms'.¹⁸¹ Like principle-based regulation (discussed below), compliance-based regulation focuses on the desired outcome rather than the means used to achieve it. This permits flexibility of approach to regulation.
- 4.111 Like responsive regulation, the first efforts by a regulator in a compliance-based system are education, cooperation and structured guidance. A compliance-based approach is about

*providing incentives and encouragement to voluntary compliance and nurturing the ability for private actors to secure compliance through self-regulation, internal management systems, and market mechanisms where possible.*¹⁸²

- 4.112 Christine Parker believes that compliance-based regulation can be expressed in seven principles:
1. identification and analysis of problems
 2. harnessing of private capacity to secure compliance through alternatives to public regulation
 3. use of process or outcome-based regulation where possible to maximise voluntary compliance
 4. provision of rewards and incentives for high/voluntary compliance
 5. informed monitoring of non-compliance
 6. dialogue and restorative justice when compliance fails, and
 7. tit-for-tat enforcement when restorative justice fails.¹⁸³
- 4.113 Compliance-based regulation also requires a strong emphasis on monitoring for non-compliance. Monitoring determines whether the system is achieving its aims.¹⁸⁴ A system that includes monitoring recognises that not all impacts are foreseeable, and that gaps and loopholes in the regulatory model can be identified using the information gathered.
- 4.114 Secondly, compliance-based regulation takes a rehabilitative approach to enforcement rather than a punitive one. Parker writes that in the face of non-compliance this approach would require an 'attempt to restore or nurture compliance rather than reverting immediately to a purely punishment-oriented approach'.¹⁸⁵
- 4.115 Critics argue that a major weakness in compliance-based regulatory theory is that in practice businesses will only do the right thing when it is in their interest to do so.¹⁸⁶ However, studies have found that this is not always the case. One US study examined whether cooperative enforcement, or punitive, sanction-based, enforcement, was a more effective means of protecting the environment. It found that there was greater success and compliance when using a cooperative approach in which a regulator worked with stakeholders to develop commitment and capacity for compliance.¹⁸⁷

Principle-based regulation

- 4.116 A consequence of compliance-based regulation is that it places great emphasis on principles that articulate the desired outcomes of any use of regulation. Scholars who support principle-based regulation suggest that regulation that relies exclusively on proscriptive rules is a creature of the past and does not have the flexibility required for regulation in the modern era.¹⁸⁸ 'Principles ... have the benefit of congruence: of communicating the regulatory objectives and promoting behaviour that will achieve those objectives.'¹⁸⁹
- 4.117 Principle-based regulation focuses on outcomes and uses overarching principles to guide the regulatory regime. It seeks to address the problems inherent in rule-based regulation by enabling the regime to respond to new issues as they arise without having to create new rules. In a rapidly changing field, such as public place surveillance, a principles-based approach can focus the aims of new regulation and provide a set of overarching standards than can adapt to new technologies and practices.
- 4.118 Principle-based approaches are already in place in state and federal information privacy laws. In its recent review of federal privacy laws, the ALRC recognised the importance of principle-based regulation when dealing with privacy.¹⁹⁰ The commission agrees with this approach and the surveillance principles described in Chapter 5 form the centrepiece of our recommendations.

- 174 Braithwaite, above n 170, 20–1.
- 175 Ayres, above n 169, 39.
- 176 Christine Parker, 'Reinventing Regulation Within the Corporation: Compliance Oriented Regulatory Innovation' (2000) 32(5) *Administration and Society* 529, 541.
- 177 Ibid 19.
- 178 Braithwaite, above n 170, 19.
- 179 Ayres, above n 169, 48–9.
- 180 Parker, above n 176, 533.
- 181 Ibid 542.
- 182 Ibid 539.
- 183 Ibid 535.
- 184 Ibid 536–7.
- 185 Ibid 539.
- 186 Ibid 534.
- 187 Ibid 538.
- 188 See eg, Julia Black, Martyn Hopper and Christa Band, 'Making a Success of Principles-Based Regulation' (2007) *May Law and Financial Markets Review* 191; Surendra Arjoon, 'Striking a Balance Between Rules and Principle-Based Approaches for Effective Governance: a Risks-Based Approach' (2003) 68(1) *Journal of Business Ethics* 53.
- 189 Black, above n 188, 195.
- 190 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008) [4.4].

A Balanced Approach to Regulation

4.119 One of the criticisms of principle-based regulation is that it leads to uncertainty and inconsistency as organisations and agencies interpret and adapt to the principles.¹⁹¹ Moreover, principles-based regulation is considered inadequate as a form of regulation on its own.¹⁹² The ALRC's approach to privacy regulation is, however, a hybrid model that relies on principles as high level objectives and uses more traditional rule-based regulation to ensure certainty and compliance.¹⁹³ The commission has adopted a similar approach to the regulation of public place surveillance.¹⁹⁴

The Victorian Guide to Regulation

4.120 The commission has also considered the Victorian Guide to Regulation. The Guide encapsulates much of the modern theoretical writing and provides a blueprint for regulatory reform in Victoria. It seeks to establish a consistent regulatory framework across the whole of the Victorian government.¹⁹⁵ The commission's recommendations will ultimately have to satisfy the Victorian Competition and Efficiency Commission (VCEC) of their value in accordance with the Guide if they are to be adopted.

4.121 The VCEC outlines characteristics of good regulatory systems. It requires a step-by-step approach that identifies the existence of a problem, the justification for government action and an assessment of whether regulation and the form of regulation chosen is the best option available to government to address the concern.

4.122 The Guide's threshold requirement is that there must be a legitimate justification for government intervention. The Guide suggests that there are at least three broad reasons for governments to choose to regulate in a particular field. They are first, in order to deal with the failure of the market to regulate an activity, secondly, to address social welfare objectives and, thirdly, to address the management of public risk.¹⁹⁶

4.123 Regulation of public place surveillance clearly falls within two of these categories. Important rights and freedoms are threatened by inappropriate, disproportionate or overly intrusive public place surveillance. This problem is exacerbated by the prevalence of surveillance use in Victoria, the increasing sophistication and capabilities of surveillance devices, and the increasing inability of current laws to effectively regulate in this area. In addition, there is a real risk of harm to vulnerable sections of the community if public place surveillance remains largely unregulated.

Is there a problem that requires intervention?

4.124 There are major shortcomings in the way we regulate public place surveillance because we have no laws specifically designed for this purpose. Commonwealth and State information privacy laws regulate public place surveillance to a limited extent only as part of general regimes that govern the collection and use of private information. The *Surveillance Devices Act 1999 (Vic)* (SDA) is of limited relevance because it is primarily concerned with the use of concealed surveillance devices in private places and with authorising and monitoring the police use of surveillance.¹⁹⁷

4.125 There is widespread concern about the lack of certainty in the existing regulatory regime. Users of surveillance frequently stated that they were unsure of what surveillance they could lawfully undertake and welcomed further guidance.¹⁹⁸ The commission's recommendations seek to balance the continuing use of surveillance with the rights of individuals who may be harmed unless surveillance is used responsibly and only when appropriate.

- 4.126 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 by misuse and overuse of surveillance in public places. Only government can balance these competing interests and take steps to discourage or prevent the inappropriate use of surveillance.
- 4.127 The harm surveillance can cause is not always easy to identify, especially when compared to other kinds of harm, such as physical injuries or damage to property. However, just because surveillance-related harm, such as invasion of privacy, is difficult to quantify, it does not mean there is no need for regulatory action to minimise the incidence of harm.¹⁹⁹
- 4.128 Some useful parallels can be drawn between the potential harm caused by unregulated use of surveillance in public places and the harm caused by various threats to the physical environment. In all of these instances, the harm may not always be immediate or easily quantifiable.²⁰⁰ Sometimes the potential harm can seem less important, or in less need of an immediate response, because 'it is perceived to be too far over the horizon'.²⁰¹ Some harms, such as the chilling effect brought about by the excessive use of surveillance in public places, might not affect an individual directly or immediately, but might still influence the way that person lives and the community uses public places. The particular activity might upset 'the balance of social or institutional power in undesirable ways'.²⁰²
- 4.129 Once the need for regulation is established, the Guide suggests that regulatory reform be characterised by the following eight features:²⁰³
1. Effectiveness: 'Regulation ... must be focused on the problem and achieve its intended policy objectives with minimal side-effects.'
 2. Proportionality: Regulatory measures must be proportional to the problem that they seek to address.
 3. Flexibility: Government should pursue a culture of continuous improvement and any new legislation should not constrain future government responses.
 4. Transparency: The development and enforcement of regulation should be transparent to the community and business sector. 'Transparency can promote learning and information-sharing within the regulatory system, and can also help to build public trust in the quality of regulation and the integrity of the process.'
 5. Consistency and predictability: Regulation needs to be consistent with other government policies and applied consistency. It should also be predictable to allow for a stable regulatory environment.
 6. Cooperation: Regulation should be developed cooperatively and aim to build a cooperative culture.
 7. Accountability: Government and enforcement agencies should be monitored with the result being reported to the public on a systemic basis.
 8. Review: Robust and transparent mechanisms for appeal should be available when regulatory action has a significant impact on an individual or business.
- 4.130 According to the Guide, each of these characteristics should be present in any new Victorian regulatory regime. They have been considered and applied to the package of reforms recommended by the commission.²⁰⁴

- 191 Julia Black, 'Managing Discretion' (Paper presented at the ALRC Conference, Penalties: Policy, Principles and Practice in Government Regulation, Sydney, 7 June 2001) 23–4.
- 192 See eg, Julia Black, 'Forms and Paradoxes of Principles Based Regulation', LSE Legal Studies Working Paper No 13/2008 (2008) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1267722> at 21 December 2009.
- 193 Australian Law Reform Commission, above n 190, 241–2.
- 194 The details of the commission's specific reform options are contained in the following chapters. Chapter 5 outlines the proposed principles to guide the use of surveillance in public places.
- 195 Department of Treasury and Finance, *Victorian Guide to Regulation* (2nd ed, 2007) 1–3.
- 196 *Ibid* 2–1, 2–2, 2–3.
- 197 Victoria, *Parliamentary Debates*, Legislative Assembly, 25 March 1999, 191–2 (Jan Murray Wade, Attorney-General).
- 198 Submissions 7, 26, 33; Consultation 11; Site Visit 16.
- 199 Solove, above n 142, 487–8.
- 200 Dan Adams, 'Climate Change and Human Rights' (Paper presented at the 2008 Human Rights Oration, Victorian Equal Opportunity and Human Rights Commission, Melbourne, 4 January 2009) 7–8.
- 201 *Ibid*.
- 202 Solove, above n 142, 488.
- 203 Department of Treasury and Finance, above n 195, 3–2.
- 204 For specific recommendations forming part of the commission's model see Chapters 5, 6 and 7.

AN OVERVIEW OF OUR RECOMMENDATIONS AND OUR APPROACH

- 4.131 The commission's conclusions about the best possible regulatory approach are guided by our extensive consultations, site visits, submissions and research. Our Consultation Paper contained a range of reform options that produced helpful responses from many organisations and individuals.
- 4.132 Our research and consultations have led us to recommend a regulatory approach that is primarily educative. The commission believes that regulation must focus on encouraging best practice use of surveillance rather than placing additional burdens on business and government.
- 4.133 The commission faced a number of challenges when developing its reform options. First, in this area 'there is no clear-cut wrongdoer, no indisputable villain whose activities lack social value'.²⁰⁵ Secondly, the capacity of the technology used to engage in surveillance in public places is constantly changing. Thirdly, it is extremely difficult to regulate most of the activities of once-off uses of surveillance devices, such as people who use mobile phones that have a range of functions.²⁰⁶
- 4.134 An approach that emphasises information collection and guidance about responsible practices is a useful first step in a field in which there has been little regulation. As technology develops and the potential for harm increases, it is important to provide guidance to users and information to the community about the use of surveillance.
- 4.135 The commission has developed a principle-based, outcome-focused approach to regulation of public place surveillance. We have devised a set of overarching principles that can be included in legislation. Those principles, which are set out in Chapter 5, seek to balance competing rights and interests.
- 4.136 The commission recommends that an independent regulator be appointed. In line with modern regulatory theory, the primary function of the independent regulator will be to work collaboratively with surveillance users. The regulator will assist users to comply with the principles and will inform the public about the operation of surveillance in public places. The commission has recommended in Chapter 5 that the independent regulator have a range of powers to guide and ensure compliance with the principles.
- 4.137 In the chapters that follow we describe other recommendations that are designed to deal with the most serious misuses of surveillance in public places. These responses include the introduction of civil penalties for breaches of the SDA, clarifying the reach of existing criminal prohibitions in the SDA, the creation of a new offence designed to deal with the most offensive uses of surveillance and two new civil causes of action for misuse of surveillance.

CONCLUSION

- 4.138 Public place surveillance offers both benefits and risks. It affects important rights. Do the risks outweigh the benefits? Which rights are paramount? The responses depend on a range of matters, including the type of public place surveillance under consideration, the purpose for which it is used, and the organisation or person conducting the surveillance.

- 4.139 Achieving a balance between the risks and benefits of public place surveillance sometimes involves personal choice. At times we must choose whether to forfeit some aspects of our privacy in exchange for one or more of the benefits of public place surveillance. Some people may, for example, be willing to give up privacy with respect to their car travel patterns in return for speedier travel on a toll road. During the recent trial phase of the x-ray body scanners at Melbourne airport people were able to decide whether to allow invasive scrutiny of their body image to avoid submitting to the alternative, a physical pat-down.²⁰⁷
- 4.140 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 increasingly foregoing our privacy not merely for convenience, but also in order to access basic services.
- 4.141 Regulation is needed in order to encourage responsible practice, to assist with those instances where choice about submitting to surveillance is illusory, and to respond effectively to gross misuse of surveillance devices. Any regulation of public place surveillance must be flexible enough to balance the many competing interests.

205 Solove, above n 142, 563.

206 Submissions 11, 13, 29, 33, 38.

207 Dan Oakes, 'Melbourne Airport Scanners "Will Show Private Parts"', (2008) *Sydney Morning Herald* (Sydney) <www.smh.com.au/news/news/airport-scanners-show-genitals/2008/10/15/1223750083412.html> at 21 January. 2009. A woman was recently barred from flying in the UK because she refused to submit to a body scan: 'Muslim Woman Barred From Flight After Refusing Body Scan' (2010) *Telegraph UK* <www.telegraph.co.uk/travel/travelnews/7358967/Muslim-woman-barred-from-flight-after-refusing-body-scan.html> at 25 March 2010.

Chapter 5

Promoting Responsible Use of Surveillance in Public Places

CONTENTS

- 84 Introduction
- 84 Principles to govern the use of surveillance in public places
- 89 An independent regulator of public place surveillance
- 90 Regulatory functions
- 90 Encouraging responsible practice
- 93 Significant surveillance users: ensuring responsible practice
- 98 Investigations and proceedings in relation to SDA breaches
- 99 The most appropriate body to regulate public place surveillance
- 101 Review of Victoria Police surveillance practices
- 103 Regulatory features not recommended at this stage
- 105 Conclusion

Promoting Responsible Use of Surveillance in Public Places

INTRODUCTION

- 5.1 This chapter contains details of the commission’s recommendations for promoting the responsible use of surveillance in public places in Victoria. We have developed an approach to regulation that is based on principles and focuses upon outcomes. The first limb of the commission’s regulatory approach is a set of overarching legislative principles to guide all users about responsible use of public place surveillance.
- 5.2 The second limb is the creation of an independent regulator who will assist users to comply with the principles and inform the public about responsible surveillance use. In this chapter we outline the range of functions and powers necessary for the regulator to fulfil these tasks, bearing in mind that the least restrictive regulatory methods are desirable. In preparing these recommendations, we have drawn upon the opinions expressed in submissions and consultations and the views of our Consultative Committee.
- 5.3 Although appropriate guidance about the responsible use of surveillance in public places is a cornerstone of our recommendations, we believe that guidance alone cannot protect people from some practices that seriously affect their privacy. Chapters 6 and 7 deal with additional regulatory measures for particularly offensive uses of surveillance.

PRINCIPLES TO GOVERN THE USE OF SURVEILLANCE IN PUBLIC PLACES

- 5.4 Victoria does not have any laws that seek to promote the responsible use of surveillance in public places. As outlined in Chapter 3, existing privacy and surveillance laws were not designed to deal with public place surveillance. Privacy laws regulate the handling of ‘personal information’¹ by agencies and large organisations. They are limited in their application to public place surveillance because common means of surveillance, such as CCTV, monitor the activities of large numbers of people who may not always be easily identifiable.
- 5.5 The *Surveillance Devices Act 1999* (Vic) (SDA) was designed to prohibit the use of covert surveillance devices primarily in private places, while also allowing law enforcement agencies to engage in such activities when authorised by judicial warrant to do so.
- 5.6 We published draft policy principles in our Consultation Paper and invited comments. Most people who expressed a view were supportive of the proposal to introduce principles to guide regulation of public place surveillance.² For example, the Federal Privacy Commissioner noted that

*a simple set of principles is an effective way to encourage users of surveillance to build privacy compliant practices into a surveillance system prior to its implementation.*³
- 5.7 Some people who made submissions were concerned that any principles should reflect the rights contained in the *Charter of Human Rights and Responsibilities Act 2006* (Vic) (the Charter), in particular the right to privacy.⁴ When refining the principles, we took account of the views expressed in submissions and considered the principles contained in federal and state privacy laws.
- 5.8 Devising general principles about the use of surveillance in public places is challenging because there are many different users of surveillance and many contexts in which it is used. What the community would consider acceptable conduct by government departments and large organisations might differ from what would be expected from individuals using surveillance devices for their own purposes. Adding to the complexity is the wide range of interests at stake.

5.9 The principles are designed to work together. Although they are expressed very generally, a primary function of the proposed regulator will be to provide users of surveillance with guidance about how each of the principles applies to them.

SIX PUBLIC PLACE SURVEILLANCE PRINCIPLES

5.10 We have devised six public place surveillance principles.

1. People are entitled to a reasonable expectation of privacy when in public places.
2. Users of surveillance devices in public places should act responsibly and consider the reasonable expectations of privacy of individuals.
3. Users of surveillance devices in public places should take reasonable steps to inform people of the use of those devices.
4. Public place surveillance should be for a legitimate purpose related to the activities of the organisation conducting it.
5. Public place surveillance should be proportional to its legitimate purpose.
6. Reasonable steps should be taken to protect information gathered through public place surveillance from misuse or inappropriate disclosure.

We explain these principles in the following paragraphs.

1. People are entitled to a reasonable expectation of privacy when in public places

- 5.11 There is increasing international acceptance of the fact that people's reasonable expectations of privacy extend to activities in public places. The notion that people can have reasonable expectations of privacy in public places has been accepted in cases arising under European and Canadian human rights instruments,⁵ and at common law in the UK and the US.⁶ The human right to privacy in the Charter is not limited to private spaces.
- 5.12 The Irish Law Reform Commission has stated that privacy is a personal right, 'following the personal space of the person'.⁷ The NSW Law Reform Commission (NSWLRC) agreed with this view, noting that 'for this reason the right is not extinguished by entry into either a public space or onto another's private property'.⁸ Some members of the Victorian parliament acknowledged the expectation of privacy in some public places, such as at the beach, when considering the SDA in 1999.⁹
- 5.13 Most people demonstrate an expectation of some privacy when in public places—for example, by wearing clothing to hide intimate areas of the body and avoiding discussion of personal matters when there is a chance of being overheard.¹⁰ In submissions and consultations most groups were of the view that individuals do have some right to privacy in public places. However, most also stated that the right to privacy is not as extensive in public places as it is in private places.
- 5.14 As technology enables ever-closer scrutiny of individuals, the view that a right to some privacy exists in public places has gained more popularity. Even when submissions suggested that little or no right to privacy in public places existed, they nevertheless acknowledged that the use of surveillance in public should be limited to some extent. It was noted that, for example, particular care should be taken before filming a private funeral on a public street.¹¹ It was also noted that permission of a child's parents should be sought before filming the child.¹²

1 Personal information is defined as being information or an opinion (including information or an opinion forming part of a database) 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: *Privacy Act 1988* (Cth) s 6 (read in conjunction with section 16B); *Information Privacy Act 2000* (Vic) s 3.

2 See eg, Consultations 1, 4, 5, 14.

3 Submission 35.

4 See eg, Submissions 5, 13, 20; Consultation 28.

5 Eg, *PG and JH v United Kingdom* (2001) IX Eur Court HR; *Aubry v Éditions Vice-Versa Inc* [1998] 1 SCR 591.

6 Eg, *Campbell v MGN Ltd* [2004] 2 AC 457; *Katz v United States* 389 US 347 (1967).

7 Ireland Law Reform Commission, *Privacy: Surveillance and the Interception of Communications* Report 57 (1998) [2.11].

8 NSW Law Reform Commission, *Surveillance: An Interim Report*, Report No 98 (2001) [4.41].

9 Victoria, *Parliamentary Debates*, Legislative Council, 11 May 1999, 524–5 (Maree Luckins); Victoria, *Parliamentary Debates*, Legislative Assembly, 22 April 1999, 551 (Rob Hulls) 555 (Victor Perton), 559 (Hurtle Lupton).

10 Nicole Moreham, 'Privacy in Public Places' (2006) 65 *Cambridge Law Journal* 606, 618.

11 Consultation 12.

12 Consultation 12.

Promoting Responsible Use of Surveillance in Public Places

5.15 Although there may be shared expectations of privacy in public places, the extent and reasonableness of those expectations differs according to context. Commentators have identified a number of factors relevant to the expectation of privacy in public places.¹³ Submissions and consultations also noted certain relevant factors. The commission's view is that the reasonableness of any expectation of privacy in public will depend on, among other things, the following factors:

- the location
- the nature of the activity being observed
- whether the activity is recorded and disseminated
- the type of surveillance used
- the identity of the person being observed (for example a public official, celebrity or a member of the public)
- whether the surveillance was harassing in nature
- whether the surveillance was covert
- whether the person specifically consented to the surveillance.¹⁴

2. Users of surveillance devices in public places should act responsibly and consider the reasonable expectations of privacy of individuals

5.16 This principle seeks to oblige surveillance users to consider the reasonable expectations of privacy of people who may be subject to that surveillance. For example, this principle should make it quite clear that the use of visual surveillance in a department store's fitting rooms to deter theft would be contrary to reasonable expectations of privacy. Consequently, it would not be responsible practice to use a visual surveillance device in this area for this purpose.

5.17 There may be situations in which the 'reasonable expectations' of privacy of individuals is not clear. In these instances surveillance users should be able to turn to the regulator for guidance about what is appropriate in the circumstances.

3. Users of surveillance devices in public places should take reasonable steps to inform people of the use of those devices

5.18 This principle seeks to ensure that members of the public are aware of when they are under surveillance. Notification reduces the potential for harm by allowing people to adjust their behaviour in response to the surveillance activity. Many submissions emphasised that people should know when they are being watched, by whom and for what purpose.¹⁵ Organisations representing Indigenous people also suggested that there should be transparency about who has access to any surveillance footage.¹⁶

5.19 What constitutes 'reasonable steps to inform people of the use' of surveillance devices will depend upon context. For example, while it is reasonable to expect a department store to have signs notifying the public that they use CCTV, 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. The regulator will be well placed to advise surveillance users about what is reasonable in their particular circumstance, and the public about what they can expect.

5.20 In determining what is reasonable, the regulator should consider the particular circumstances of each type of surveillance use. For example, most CCTV operators should not be required to place signs under every single camera in operation. It may be more appropriate to use a limited number of well-placed signs, including a visual depiction of a CCTV camera where appropriate. Some uses of surveillance (for example public filming by a clearly identifiable media crew) will constitute reasonable notice without the provision of any extra signage. Further, the regulator should assist users to ensure that the economic burden of providing notice does not outweigh the potential benefits in each particular circumstance.

4. Public place surveillance should be for a legitimate purpose related to the activities of the organisation conducting it

5.21 This principle seeks to ensure that organisations and agencies do not utilise surveillance in a way that is arbitrary or unnecessarily intrusive. In our preliminary consultations many groups supported this principle.¹⁷ The view was expressed that there should be a valid reason for surveillance, and that users should have to justify their practices.¹⁸

5.22 What constitutes a 'legitimate purpose' will vary according to the circumstances. 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.¹⁹

5.23 The NSWLRC identified the following legitimate uses of public place surveillance:

- protection of the person
- protection of property
- protection of the public interest
- a catch-all category, 'protection of a legitimate interest'.²⁰

5.24 Further, the purpose must be related to the activities of the organisation. The NSWLRC noted that surveillance cameras in a casino were not being used in a manner appropriate to their purpose when zooming in on female patrons.²¹

5. Public place surveillance should be proportional to its legitimate purpose

5.25 This principle seeks to ensure that the means of surveillance employed by an organisation is proportionate to the legitimate purpose for which it is used. Excessively intrusive surveillance should be used only for particularly important purposes. For example, a highly intrusive form of surveillance such as an x-ray body scanner may be justifiable when designed to protect individuals from grave physical harm, but its use to avoid minor loss of property is not likely to be proportionate to its purpose. The principle of proportionality means that a user of surveillance ought to use the least privacy-intrusive means of achieving their purpose.²²

5.26 The European Human Rights Convention has been interpreted to require proportionality between the surveillance practice and the purpose it seeks to achieve.²³ A study into the social and political impacts of CCTV in European cities recommended allowing video surveillance in public places for only a limited set of clearly defined purposes, and making surveillance use transparent.²⁴

13 See Law Reform Commission [Ireland], *Privacy: Surveillance and the Interception of Communications*, Report 57 (1998) [2.13]–[2.19]; Moreham, above n 10, 620.

14 These factors are outlined further in our Consultation Paper.

15 Roundtable 29.

16 Roundtable 28.

17 Roundtables 1, 2, 9, 19, 29.

18 Roundtable 18.

19 Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005) [3.47].

20 NSW Law Reform Commission, above n 8.

21 Ibid [4.47].

22 Victorian Law Reform Commission, above n 19 [3.50].

23 *Peck v United Kingdom*, 44647/98 [2003] I Eur Court HR 44, [76].

24 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 UK.

Promoting Responsible Use of Surveillance in Public Places

5.27 Given the many situations in which surveillance in public places occurs, it is not possible to describe in general terms those surveillance activities that may be proportional in particular circumstances. Instead, it is hoped this principle will encourage surveillance users to assess their practices and consider whether there are less intrusive ways to achieve the same purpose. The regulator will be well placed to issue guidelines and to assist individual users of surveillance.

6. Reasonable steps should be taken to protect information gathered through public place surveillance from misuse or inappropriate disclosure

5.28 This principle seeks to ensure that users of public place surveillance act responsibly by safeguarding any information they gather so that innocent people are not harmed by its misuse or disclosure without good cause.

5.29 Surveillance users have a wide variety of procedures in place concerning the handling, storing and sharing of information. Some users of CCTV systems, for example, keep all footage in a secure room, allow access only to designated staff and have strict protocols in place for the provision of footage to external parties. The commission considers this to be best practice. Other users stream their footage to monitors that may be viewed by a large number of people, and have no protocols in place for the release of footage to external parties.

5.30 This principle, which draws on existing information privacy principles, is designed to discourage the misuse of information obtained by surveillance. As noted in one submission, these principles are intended to operate in a way that expands upon, but complements, the existing information privacy laws because those laws do not effectively regulate the use of all information collected by surveillance, such as material captured by CCTV.²⁵

RECOMMENDATIONS

1. The Victorian parliament should enact new laws that promote the responsible use of surveillance devices in public places.
2. The legislation should include the following guiding principles.
 1. People are entitled to a reasonable expectation of privacy when in public places.
 2. Users of surveillance devices in public places should act responsibly and consider the reasonable expectations of privacy of individuals.
 3. Users of surveillance devices in public places should take reasonable steps to inform people of the use of those devices.
 4. Public place surveillance should be for a legitimate purpose related to the activities of the organisation conducting it.
 5. Public place surveillance should be proportional to its legitimate purpose.
 6. Reasonable steps should be taken to protect information gathered through public place surveillance from misuse or inappropriate disclosure.

AN INDEPENDENT REGULATOR OF PUBLIC PLACE SURVEILLANCE

- 5.31 The commission believes there should be an independent regulator to guide responsible use of public place surveillance in Victoria. The primary roles of the regulator would be to promote the responsible use of surveillance in public places by providing practical guidance to surveillance users, and to keep the government and the people of Victoria fully informed of rapidly changing technology.
- 5.32 Currently, no regulator has specific responsibility for monitoring the use of surveillance in public places. The Victorian and Federal Privacy Commissioners' existing responsibilities in relation to public place surveillance in Victoria are limited. The Commissioners have oversight roles in relation only to the personal information held by public agencies and large organisations. Although other regulators, such as the Director of Liquor Licensing,²⁶ have some responsibilities in relation to public place surveillance, their oversight of this area is incidental to their primary functions and involves only particular users of surveillance.
- 5.33 In our Consultation Paper we suggested the creation of a regulator to monitor public place surveillance in Victoria. There was widespread support for this proposal.²⁷ Significantly, many surveillance users said they would benefit from guidance on how to conduct public place surveillance responsibly.²⁸
- 5.34 Many of the surveillance users we consulted favoured a regulatory regime that is not intrusive or prescriptive and which emphasises the importance of educating surveillance users about responsible practices and privacy protection.²⁹ Surveillance users should be encouraged to work with a regulator to ensure that they are conducting surveillance responsibly and in accordance with public place surveillance guidelines.
- 5.35 The UK government has recently taken the first step down this path. As a result of its 2007 report on a national CCTV strategy, the Home Office has established an interim independent regulator for CCTV in the UK. The regulator has 12 months to draft recommendations to the Minister for Home Affairs on how CCTV should be regulated.³⁰ The regulator is required to raise public awareness, set standards and establish a complaints process.
- 5.36 A broadly similar regime to that proposed by the commission was introduced federally in 1999 under the *Equal Opportunity for Women in the Workplace Act 1999* (Cth) (EOWWA),³¹ which established a regulator to promote equal opportunity for women in the workplace. That regime emphasises a facilitative rather than a punitive approach to compliance.³² The primary role of the regulator is to provide advice to employers, to undertake research, and to promote understanding and acceptance of the equal opportunity principle.³³
- 5.37 Under the Act, all employers of more than 100 people must develop a program for fostering equal opportunities for women, and report outcomes to the regulator.³⁴ Where they fail to do so, the regulator may report them to the Minister.³⁵
- 5.38 Although the regime covers government and private employers, it avoids imposing an undue regulatory burden on business by exempting employers with less than 100 employees and by keeping compliance costs to a minimum.³⁶

25 Submission 14.

26 Also the Commissioner for Law Enforcement and Data Security, the Victorian Commission for Gambling Regulation and the Special Investigations Monitor.

27 See eg, Submissions 2, 5, 7, 9, 11, 12; Forums 1, 5; Consultations 5, 9, 11, 15, 17.

28 Including Submissions 7, 26, 28, 33; Consultation 11; Site Visits 10, 16.

29 Submissions 7, 11, 30, 33; Forum 1; Consultations 8, 14; Site Visit 10.

30 See *Briefing 15.12.09: National CCTV Oversight Body*, The National CCTV Strategy Board, Home Office <www.crimereduction.homeoffice.gov.uk/cctv/cctv_oversight_body_b.pdf> at 20 January 2010.

31 A modified version of the *Affirmative Action (Equal Opportunity for Women) Act 1986* (Cth).

32 Explanatory Memorandum, *Equal Opportunity for Women in the Workplace Amendment Bill 1999* (Cth) 1.

33 *Equal Opportunity for Women in the Workplace Act 1999* (Cth) s 10.

34 *Equal Opportunity for Women in the Workplace Act 1999* (Cth) ss 3, 6, 13.

35 *Equal Opportunity for Women in the Workplace Act 1999* (Cth) s 19.

36 Explanatory Memorandum, *Equal Opportunity for Women in the Workplace Amendment Bill 1999* (Cth) 1–2.

Promoting Responsible Use of Surveillance in Public Places

- 5.39 The level of compliance with the Act is significant—the 2008 annual report listed 12 non-compliant employers and noted that there were 2501 compliant employers. The report also noted that public feedback about the scheme was overwhelmingly positive.³⁷
- 5.40 The commission is of the view that a broadly similar model is appropriate for the regulation of public place surveillance.

RECOMMENDATION

3. A regulator should be responsible for the oversight of public place surveillance in Victoria.

REGULATORY FUNCTIONS

- 5.41 Responsive regulation requires a suite of tools for the regulator when encouraging compliance with best practice guidelines. We have designed a multifaceted regime that places emphasis on education and encouragement, and moves to more punitive enforcement mechanisms only as a last resort.
- 5.42 First, the regulator should have responsibility for monitoring surveillance use and technology, and for educating surveillance users and the general community about their rights and responsibilities. The development of best practice guidelines to aid users of public place surveillance is central to this role. We discuss these functions below under ‘Encouraging responsible practice’.
- 5.43 Secondly, it is the commission’s view that the regulator should work closely with significant government and private users of public place surveillance to ensure they employ best practice standards. This should include reviewing advice prepared by the users and advising on any areas for improvement, examining their surveillance practices where appropriate, and reporting findings to parliament. We discuss these functions below under ‘Significant surveillance users: ensuring responsible practice’.
- 5.44 Thirdly, the commission is of the view that it is appropriate for the regulator to seek civil penalties for the principal offences in the *Surveillance Devices Act 1999* (Vic) when this course is preferable to criminal prosecutions. This is discussed below and further in Chapter 6.

ENCOURAGING RESPONSIBLE PRACTICE

- 5.45 In order to encourage responsible practice by all public place surveillance users, the commission recommends that the regulator should be responsible for
- researching and monitoring surveillance technology and the use of surveillance in public places
 - educating, providing advice and promoting understanding of laws and best practice in relation to public place surveillance
 - developing and publishing best practice guidelines to illustrate appropriate use of public place surveillance technology.

RESEARCH AND MONITORING

- 5.46 Public place surveillance is used extensively in Victoria and its use has increased markedly in the past few years. Nevertheless, there is a distinct lack of data about the precise extent of its use, including what types of devices are used, who uses them, and for what purposes.

5.47 In our Consultation Paper we suggested that an appropriate regulator be given responsibility for researching and monitoring the use of surveillance technologies. There was widespread support for this proposal.³⁸ A thorough understanding of all aspects of public place surveillance is central to effective regulation. The information gathered will provide a base for educational campaigns to promote responsible use.

- 5.48 The commission is of the view the regulator should be responsible for
- collecting information and conducting empirical research about surveillance practices in Victoria
 - monitoring the operation of existing and proposed regulatory standards and codes
 - monitoring the operation of the law in Australia and elsewhere
 - monitoring the development of technology in order to ensure that appropriate regulatory regimes are in place
 - identifying and monitoring regulatory schemes that require, or have an impact on, the use of surveillance in public places (for example, licensing regimes for liquor, gaming, private security and private investigators) and ensuring these schemes offer consistent privacy protection
 - reviewing Australian Standards relating to design and use of CCTV and other surveillance technologies.

EDUCATING, PROVIDING ADVICE AND PROMOTING UNDERSTANDING OF LAWS AND BEST PRACTICE

5.49 Views expressed in consultations and submissions indicate there is a widespread lack of understanding (both within the general community and among users of surveillance) of many aspects of public place surveillance. It was, for example, apparent that the public is not well informed about the nature and extent of public place surveillance that is conducted in Victoria. There appears to be a lack of awareness on the part of users of surveillance devices about existing regulation.³⁹ Submissions and consultations noted the need for more clarity and certainty about the law regulating the use of public place surveillance.⁴⁰

5.50 Submissions and consultations supported the provision of education about public place surveillance.⁴¹ Many users indicated a wish for more guidance about how to conduct surveillance responsibly. One submission noted, for example, that increased awareness of surveillance technology would 'enhance the deterrent potential of surveillance ... use'.⁴²

5.51 One of the primary roles of the proposed regulator should be to ensure users of surveillance understand how to act responsibly and to follow best practice. The regulator should also be responsible for ensuring that the Victorian public is aware of the extent of public place surveillance and of their rights if surveillance is misused.

DEVELOPING AND PUBLISHING BEST PRACTICE GUIDELINES

5.52 Surveillance users should be given practical guidance about how to comply with the public place surveillance principles. In our Consultation Paper we suggested that a regulator could be responsible for devising guidelines. In submissions there was strong support for either voluntary standards or mandatory codes. Many users supported the introduction of voluntary standards.⁴³ It was noted that the introduction of a mandatory regime at this stage might place too great a burden on surveillance users.⁴⁴

37 Equal Opportunity for Women in the Workplace Agency, *Annual Report (2008–09)* 16.

38 Submissions 5, 9, 11, 12, 14, 26, 29, 33, 34, 36, 40, 42.

39 Consultations 18, 26; Site Visits 10, 17, 18.

40 Submissions 5, 33; Consultation 11; Site Visits 3, 10, 17. There was only one submission that expressed strong disagreement with having any new form of regulation, and this submission did so specifically in relation to that which might limit CCTV use in shopping centres: Submission 22.

41 Submissions 5, 7, 11, 12, 14, 29, 30, 33, 34; Forum 1; Consultations 5, 8, 14.

42 Submission 5.

43 Consultations 7, 27; Site Visit 10.

44 Submission 16.

Promoting Responsible Use of Surveillance in Public Places

5.53 Other submissions expressed the view that standards may not have much practical effect if they are not enforceable.⁴⁵ The Victorian Privacy Commissioner, for example, noted:

While the introduction of voluntary standards could be perceived to be an initial 'light touch' regulatory action ... in my view the rights and interest at stake are of such importance and the scope, extent and nature of public place surveillance is already so overwhelming that some form of mandatory regulation is required.⁴⁶

5.54 The commission proposes the adoption of voluntary standards accompanied by an obligation upon major users of public place surveillance to provide advice to the regulator about their compliance with those standards. The regulator should develop, in consultation with users, best practice guidelines for specific surveillance technologies, such as sophisticated CCTV systems, ANPR, body-scanners and biometrics.⁴⁷ This is the most appropriate way to provide users of surveillance with practical guidance about how to comply with public place surveillance principles. The guidelines would encourage users to conduct public place surveillance responsibly while also protecting their own interests. They would also provide the community with an understanding of their rights in relation to public place surveillance.

5.55 In 2009 the New Zealand Privacy Commissioner published *Privacy and CCTV*, guidelines to help businesses ensure that their use of CCTV was compliant with their obligations under the *Privacy Act 1993* (NZ).⁴⁸

5.56 The New Zealand guidelines advise CCTV users to

- clearly identify whether CCTV is appropriate and, if so, for what purposes
- develop a business plan for its use
- consult with affected people if appropriate
- choose equipment to achieve the desired aims with minimal invasion of privacy, and, where possible, use privacy enhancing technologies
- erect signage to alert the public to the use of cameras and train staff to answer questions about it
- limit the hours when footage is collected, and only retain footage as long as necessary to achieve the stated purposes
- ensure that the footage is stored securely and protected from unauthorised access.⁴⁹

5.57 Some individual users of surveillance and industry groups have developed their own CCTV standards. VicRoads, Crown Casino, the Department of Transport, Melbourne City Council and Victoria Police have internal guidelines that deal with specific aspects of surveillance use.⁵⁰ Victoria Police has arrangements with some local councils concerning access, use and storage of council CCTV footage.⁵¹ Victoria Police noted that the protocols it has with Melbourne City Council work well and could be applied in other areas.⁵²

5.58 Some of the matters that could be included in Victorian CCTV guidelines, bearing in mind the public place surveillance principles, are

- careful consideration of the need to install a public place CCTV system, including, where appropriate, consultation with communities likely to be affected
- assurance 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
- the taking of active measures, such as monitoring of staff responsible for the use of the surveillance system, in order to minimise privacy invasion
- regular evaluation of surveillance practices to determine if they continue to be justified and proportionate
- assurance that information is protected from misuse or disclosure without good cause.

5.59 The regulator should consult surveillance users, key stakeholders and the broader community when developing guidelines about particular forms of public place surveillance.⁵³ The regulator should also consider existing guidelines in other countries, such as the CCTV guidelines developed by the New Zealand Privacy Commissioner, and the guidelines followed by Victorian users of surveillance, such as those developed by the Melbourne City Council.

SIGNIFICANT SURVEILLANCE USERS: ENSURING RESPONSIBLE PRACTICE

5.60 Although the regulator should encourage all users of public place surveillance to adopt best practice standards, some significant users of surveillance could be assisted by working collaboratively with the regulator to create guidelines for their own particular activities. The regulator should have additional functions in relation to significant users which include

- reviewing advice prepared by significant users about their use of public place surveillance and compliance with laws and best-practice guidelines
- examining the practices of significant users
- advising significant users of any failure to comply with laws and best practice guidelines.

In the following paragraphs we describe 'significant users' of public place surveillance and discuss the relevant functions of the regulator.

SIGNIFICANT USERS OF PUBLIC PLACE SURVEILLANCE

5.61 There are many surveillance users in Victoria. For example, users of CCTV range from large organisations with sophisticated systems (such as government departments and sporting and entertainment venues) to small businesses (such as convenience stores) with systems of limited capacity.

5.62 The more significant users of public place surveillance should be required to work cooperatively with the regulator to integrate best practice standards into their own practices. To ensure proper accountability, significant users should be made accountable for their compliance with public place surveillance laws and best practice guidelines. Such a scheme would be similar that under federal affirmative action legislation, outlined above.

45 Submissions 7, 14, 27, 29, 33, 34, 36, 39, 40; Consultations 5, 9.

46 Submission 29.

47 These technologies are described in detail in Chapter 2.

48 Privacy Commissioner [New Zealand], 'Privacy and CCTV: A Guide to the Privacy Act for Businesses, Agencies and Organisations' (2009) <www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/Privacy-and-CCTV-A-guide-October-2009.pdf> at 23 November 2009.

49 Ibid.

50 Consultations 4, 10, 25; Site Visits 1, 13.

51 Submission 4; Consultations 19, 27; Site Visit 10.

52 Consultation 19.

53 This was supported in submissions. See Submissions 4, 16, 33, 35, 36, 39.

Promoting Responsible Use of Surveillance in Public Places

5.63 The commission believes the following users of public place surveillance should be subject to additional accountability mechanisms:

- public authorities
- 'significant private users' of public place surveillance.

Public authorities

5.64 Bodies that exercise the power of the state (public authorities) should be held to the highest standards of compliance with laws and guidelines concerning public place surveillance. The term 'public authority' is defined in the Charter to include bodies such as government departments, statutory agencies, local government and entities performing functions of a public nature on behalf of a government body.⁵⁴ The commission believes these users of public place surveillance should be required to work collaboratively with a regulator to strive for best practice. This will increase accountability of government use of surveillance and will give the regulator the opportunity to provide advice to parliament about the use of public place surveillance in Victoria.

5.65 Government agencies were among the most significant users of surveillance we consulted. Many government agencies have large, sophisticated surveillance systems that monitor activities in the streets, in public housing estates and on public transport. These systems have the capacity to record private, and potentially sensitive, information. It is important that there are appropriate safeguards concerning the way public authorities handle this information.

5.66 As described in Chapter 4, public authorities are required to give effect to privacy rights, as well as other rights, under the Charter. Adoption of best practice guidelines will ensure that agencies are meeting their obligations under the Charter. Demonstration of government compliance with best practice guidelines will also provide leadership to other users of public place surveillance.

5.67 Many public authorities already have processes in place to comply with a range of best practice guidelines and to respond to their numerous reporting requirements. Furthermore, a number of public authorities already have their own internal protocols concerning their use of public place surveillance. Some, such as Melbourne City Council, clearly follow current best practice in this area. Compliance with protocols of this nature is not expensive, especially when contrasted with the resources necessary to implement and operate a sophisticated surveillance system. Some public authorities, however, do not have appropriate protocols in place concerning their use of public place surveillance. In these cases the regulator should work with the authority to develop appropriate procedures.

5.68 When the regulator considers the use of public place surveillance is so insignificant as not to warrant additional accounting mechanisms, we believe that the regulator should have the power to exempt the public authority from additional accountability mechanisms until such time as the authority's use of surveillance changes.

Significant private users of public place surveillance

5.69 In order to ensure that surveillance is conducted responsibly throughout Victoria additional accountability mechanisms should not be limited to public authorities. Many private users—including private transport operators, sports and entertainment venues and large shopping centres—use such sophisticated public place surveillance systems that they could be misused, and the resulting potential harm could be considerable.

- 5.70 Significant private sector users of public place surveillance are generally larger organisations who will be able to carry the small burden of additional accountability mechanisms. Further, as with major government users, the resources used to fulfil these would be very small when compared to the resources used to implement and operate a sophisticated surveillance system. These significant private sector users will also benefit from the guidance and advice about best practice that would be available from the regulator.
- 5.71 The commission thinks that small users of public place surveillance, with relatively unsophisticated systems, such as a CCTV system in a convenience store, should not be burdened with these obligations at this stage. Such surveillance users should be encouraged to comply with best practice guidelines and they should have the opportunity to seek advice from the regulator.
- 5.72 In other regulatory schemes where it has been necessary to distinguish some private users from others, legislators have typically marked a distinction by the organisation's size—either by its annual turnover,⁵⁵ or by number of employees.⁵⁶ We have found these distinctions are less useful in relation to the use of surveillance in public places. Our consultations revealed that some very small organisations operate sophisticated surveillance systems⁵⁷ and, conversely, not all large organisations conduct significant public place surveillance.
- 5.73 The commission believes that a different approach should be taken in order to determine which private organisations should be considered 'significant users' of surveillance. Factors other than the size of the organisation should be taken into account. Such factors could include
- the sophistication or capacity of the surveillance system used
 - the invasiveness of the surveillance technology used (potentially, all users of the most invasive forms of surveillance)
 - the percentage or amount of public place under surveillance
 - the regulatory burden of any additional accounting requirement on the user.
- 5.74 The commission acknowledges the difficulties that arise when attempting to distinguish 'significant users' from other users of surveillance. Consequently, resorting to the approaches of other regimes may be a useful starting point. For example, the following organisations could be classified as significant users of public place surveillance:
- all organisations with a turnover of at least \$3 million
 - all major sporting and entertainment venues
 - all organisations with a primary purpose of conducting surveillance
 - other organisations or classes of organisations nominated by the regulator, including those using particularly invasive forms of surveillance.
- 5.75 Any users that fall within these broad categories should be exempted where they can demonstrate they are not significant users of public place surveillance.
- 5.76 The commission believes the Victorian Government, working in conjunction with the regulator, is best placed to determine which organisations are 'significant private users' for the purposes of the proposed regime.

54 The commission adopts the meaning of 'public authority' set out in section 4 of the *Charter of Human Rights and Responsibilities Act 2006* (Vic).

55 See eg, the *Privacy Act 1988* (Cth), in which businesses with a turnover of \$3 million or less are exempt from the operation of the national privacy principles.

56 See eg, the *Equal Opportunity for Women in the Workplace Act 1999* (Cth), in which employers with less than 100 employees are exempt from the operation of the Act.

57 See eg, Site Visit 22.

Promoting Responsible Use of Surveillance in Public Places

REVIEWING ADVICE PREPARED BY SIGNIFICANT USERS OF PUBLIC PLACE SURVEILLANCE

- 5.77 It is the commission's view that significant users of public place surveillance devices should provide regular advice to the regulator about their use of surveillance in public places, including their compliance with law and best practice guidelines. One of the functions of the regulator would be to provide users with a template for the provision of advice, so that users can understand what is expected of them. The regulator would also be responsible for reviewing advice and providing reports to government.
- 5.78 A requirement to report is a feature of a number of other educative regulatory regimes. The EOWWA, for example, requires all organisations with more than 100 employees to produce a workplace program and report to the regulator.⁵⁸ The regulator has developed a number of educational tools and other resources to assist employers when making their reports.⁵⁹
- 5.79 Similar reporting requirements are already used in Victoria. Victorian public sector bodies are required to prepare action plans outlining their initiatives to make workplaces accessible for people with disabilities, and to report on the implementation of their plans.⁶⁰ The Victorian Government's policy, *A Fairer Victoria 2006*, requires all departments to develop a cultural diversity plan.⁶¹ Likewise, the government's *Our Environment Our Future* policy requires all departments and agencies to report on their integration of the government's Environmental Sustainability Framework.⁶² The commission is of the view that broadly similar reporting requirements are appropriate for significant users of public place surveillance. The level of detail required in reports should be determined by the regulator, and would vary according to the class of user and type of surveillance technology.

EXAMINING THE PRACTICES OF SIGNIFICANT USERS OF PUBLIC PLACE SURVEILLANCE

- 5.80 The commission recommends that the regulator be responsible for examining the practices of significant users of public place surveillance.
- 5.81 This is a similar function to one held by the Victorian Privacy Commissioner. The Commissioner has a responsibility to 'examine the practices of an organisation with respect to personal information maintained by that organisation for the purpose of ascertaining whether or not the information is maintained according to the Information Privacy Principles'.⁶³ The Privacy Commissioner has the 'power to do all things that are necessary or convenient to be done for or in connection with the performance of his or her functions'.⁶⁴
- 5.82 It is envisaged that the surveillance regulator may examine the practices of significant surveillance users on a systematic basis (that is, routinely, by class of user or type of device). The regulator may wish to examine a particular surveillance user if it did not provide advice to an appropriate standard, or if the advice was unsatisfactory in some way. An examination may also be triggered by the regulator's research, or in response to a report by a member of the public about the surveillance practices of a particular user.

ADVISING OF A SIGNIFICANT USER'S FAILURE TO COMPLY

- 5.83 In line with the responsive regulatory approach outlined in the previous chapter, the commission believes that the regulator should have a number of options when a significant user of public place surveillance fails to comply with the law or with best practice guidelines.

- 5.84 As a first step, the regulator should have the power to advise a significant user of any failure to comply with best-practice guidelines and to require that user to provide advice about action taken to remedy that failure.
- 5.85 The Victorian Privacy Commissioner is currently empowered to serve a compliance notice on an organisation if it appears it has acted in a way that 'constitutes a serious or flagrant contravention' of an information privacy principle.⁶⁵ It is an offence not to comply with a compliance notice.⁶⁶
- 5.86 The proposed power for the surveillance regulator differs from this existing compliance notice power because failure to rectify the breach following advice from the surveillance regulator would not be an offence. However, failure by a significant user to remedy the breach could result in an adverse report to parliament, which is discussed in more detail below.
- 5.87 Where it comes to the attention of the regulator that a surveillance user may have breached the SDA, the regulator should have the power to commence civil penalty proceedings or refer the matter to the police for criminal action. These options are discussed later in this chapter and in Chapter 6.

REPORTING TO PARLIAMENT

- 5.88 The commission recommends that the regulator provide an annual report to parliament about the use of surveillance in public places in Victoria and about any developments in technology that may require separate regulation.
- 5.89 Such a report should include advice about the users of public place surveillance, the devices that are used and the reasons for their use. Much of this information could be drawn from the advice provided by significant users of public place surveillance.
- 5.90 The regulator should also be responsible for reporting about changes to surveillance technologies, and the potential risks and benefits that may arise from the use of these technologies. The regulator should advise government about whether current legislative frameworks are adequate to deal with such changes. In addition to providing legislators with valuable information, these reports will also serve the function of informing the wider community about best practice use of surveillance in public places.
- 5.91 The Federal Privacy Commissioner is empowered to provide the Minister with a report relating to an inquiry or audit into any matter related to his or her functions, which the Minister must table in parliament.⁶⁷ 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.⁶⁸ The Victorian Privacy Commissioner currently has limited reporting powers. The Commissioner may report to the Attorney-General in relation to some of the commission's functions only, and the Act does not require the Attorney-General to table the reports in parliament.⁶⁹ The commission is of the view that the proposed surveillance regulator should have similar reporting powers to those possessed by the federal and NSW Privacy Commissioners.

- 58 *Equal Opportunity for Women in the Workplace Act 1999* (Cth) s 13.
- 59 Australian Government, *Equal Opportunity for Women in the Workplace Agency*, <www.eowa.gov.au/Reporting_And_Compliance/The_Quick_Guide.asp#06> at 7 December 2009.
- 60 *Disability Act 2006* (Vic) s 38.
- 61 Department of Premier and Cabinet, *A Fairer Victoria* <[www.dse.vic.gov.au/DSE/nrence.nsf/LinkView/C50F9AEFF496CEA8CA256FE800232FE1E2176756455B21FFCA256E57007C82CF](http://www.dpc.vic.gov.au/CA256D8000265E1A/page/Listing-Government+Initiatives-A+Fairer+Victoria++The+Victorian+Government%27s+social+policy+action+plan!OpenDocument&1=-&2=-&3=->at 8 December 2009.</p>
<p>62 Department of Sustainability and Environment, <i>Victoria's Environmental Sustainability Framework: Our Environment Our Future</i> (2005) < at 8 December 2009.
- 63 *Information Privacy Act 2000* (Vic) s 58(g).
- 64 *Information Privacy Act 2000* (Vic) s 59.
- 65 *Information Privacy Act 2000* (Vic) s 44(1)(a).
- 66 In the case of a body corporate, the offence attracts 3000 penalty units; in any other case 600 penalty units. *Information Privacy Act 2000* (Vic) s 48.
- 67 *Privacy Act 1988* (Cth) s 32(1), (3).
- 68 See *Privacy and Personal Information Protection Act 1998* (NSW) s 65(1)–(2).
- 69 *Information Privacy Act 2000* (Vic) s 58.

Promoting Responsible Use of Surveillance in Public Places

Reporting non-compliance with best practice guidelines by significant users

- 5.92 Reporting is used as a successful compliance tool in a number of federal and state regimes. For example, reporting is the ultimate sanction for continued non-compliance with laws under the EOWWA regime discussed above. The NSW Food Authority publishes a 'Register of Penalty Notices', a public list of details of cafes and restaurants that have failed to comply with food standards.⁷⁰ In its first three weeks of operation, the website was accessed 25 000 times⁷¹ and 1.5 million times during its first year.⁷² Victorian legislators plan to implement a similar scheme in the food industry from mid 2010.⁷³
- 5.93 The commission takes the view that the most appropriate way to deal with routine non-compliance by significant users of surveillance with best practice guidelines is by reporting these users to parliament.
- 5.94 Reputation is important to both the government and the private sectors. To government, a loss of reputation raises obvious political risks. Studies have shown that damage to reputation is also a significant concern for private organisations.⁷⁴ Modern regulatory theorists have noted that public reporting can help add to a 'culture of compliance'⁷⁵ with the particular regime in question.

INVESTIGATIONS AND PROCEEDINGS IN RELATION TO SDA BREACHES

- 5.95 A greater range of regulatory measures should be available to control the use of surveillance in Victoria. In Chapter 6 we outline the rationale for introducing civil penalties, as an alternative to criminal penalties, into the SDA. We recommend that the surveillance regulator be responsible for investigating potential breaches of the SDA, and instituting civil penalty proceedings in the Victorian Civil and Administrative Tribunal (VCAT) where appropriate.
- 5.96 At present, Victoria Police is responsible for investigating and prosecuting breaches of the SDA. The commission is aware of only four successful prosecutions for breach of the Act since its inception on 1 January 2000 (all in relation to unlawful uses of optical surveillance devices).⁷⁶ The Victorian Privacy Commissioner noted the potential for a conflict of interest to arise in this role, particularly as police are one of the major users of surveillance; they also often use the information captured by other users.⁷⁷
- 5.97 The commission's recommendation that a regulator be made jointly responsible for investigating potential breaches and initiating proceedings under the SDA is consistent with recommendations of the ALRC. The ALRC recommended amendments to the Privacy Act to allow the federal 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.⁷⁸
- 5.98 The commission recommends that the regulator be provided similar investigative powers to those of other bodies responsible for initiating civil penalty proceedings, for example the Australian Security Investment Commission (ASIC) or the Australian Competition and Consumer Commission (ACCC).⁷⁹ ASIC has the power to seek a wide range of civil remedies, for example to prevent or contain damage to corporate or individual assets, assist in the return of assets or to obtain damages.⁸⁰ Similarly, under the *Trade Practices Act 1974* (Cth), the ACCC may institute a civil proceeding in the Federal Court for the recovery of a monetary penalty for a potential breach of certain provisions of the Act.⁸¹

RECOMMENDATIONS

4. The regulator should have the following functions in relation to public place surveillance:
 - a. research and monitoring, including use, technologies and current laws
 - b. educating, providing advice and promoting understanding of laws and best practice
 - c. developing and publishing best practice guidelines
 - d. reviewing advice prepared by public authorities and significant private users of public place surveillance
 - e. examining the practices of public authorities and significant private users in relation to their public place surveillance practices
 - f. advising a public authority or significant private organisation of any failure to comply with laws and best practice guidelines
 - g. investigating and taking civil proceedings in relation to potential breaches of the SDA
 - h. reporting to the Minister on an annual basis on any matters in relation to any of its functions, including any failure by public authorities and significant organisations to comply with advice under paragraph (f).
5. Public authorities and significant private users should be required to provide advice to the regulator annually on their compliance with public place surveillance guidelines in relation to designated surveillance devices.
6. The Victorian Government should define 'significant private user' for the purposes of the regulatory regime.
7. In addition to any other powers conferred on the regulator by legislation, the regulator should have the power to do all things necessary or convenient for, or in connection with, the performance of the functions of the regulator.⁸²
8. In addition to his or her annual reporting function, the regulator should also have the power to report formally to the relevant Minister about any matters relating to his or her functions. The Minister should be required to table all reports provided by the regulator in parliament.

THE MOST APPROPRIATE BODY TO REGULATE PUBLIC PLACE SURVEILLANCE

- 5.99 The commission believes it is more appropriate to extend the functions of an existing regulator to regulate surveillance in public places than to create a new regulator. This approach is consistent with the Victorian Government's commitment to devise regulatory options that are as cost-effective as possible and that minimise the regulatory burden on agencies and organisations.⁸³
- 5.100 In our Consultation Paper we sought submissions about the most appropriate body to regulate public place surveillance. We suggested that the Victorian Privacy Commissioner appeared to be an obvious choice to exercise regulatory functions in relation to public place surveillance because of the Commissioner's expertise in protecting privacy.

- 70 Available at NSW Food Authority, *Food Safety Offences* <www.foodauthority.nsw.gov.au/aboutus/offences/> at 18 November 2009.
- 71 NSW Food Authority, *Name and Shame Website Scores 25,000 Hits in Three Weeks* (2008) <www.foodauthority.nsw.gov.au/aboutus/media-releases/mr-23-Jul-08-name-and-shame-website-hits/> at 18 November 2009.
- 72 Food Safety Australia, *Name and Shame List Nearly a Year Old* (2009) <www.foodsafety.edu.au/news/2009/06/name-shame-list-nearly-a-year-old/> at 18 November 2009.
- 73 Food Amendment (Regulation Reform) Bill 2009 (Vic). Note that the ACCC may soon have a name and shame power in the form of a right to issue public warning notices: Trade Practices Amendment (Australian Consumer Law) Bill 2009 (Cth) cl 86DA.
- 74 Brent Fisse and John Braithwaite, *The Impact of Publicity on Corporate Offenders* (1983), 247.
- 75 *Ibid* 2–3.
- 76 See Steve Butcher, 'Man May Face Jail For Pointing Camera at Woman in Toilet', *The Age* (Melbourne), 4 March 2010, 10; Mark Russell, 'Privacy Threatened by Rise in Hidden Cameras', *The Age* (Melbourne), 30 September 2007, 2; 'Former Drama Teacher Pleads Guilty to Porn Charges', *The Age* (Melbourne), 1 March 2010, 6.
- 77 Submission 29.
- 78 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report* 108 (2008) Rec 50–2.
- 79 See powers under the *Australian Securities and Investment Commission Act 2001* (Cth) s 13 and the *Trade Practices Act 1974* (Cth) s 155.
- 80 See eg, powers under the *Financial Services Reform Act 2001* (Cth).
- 81 *Trade Practices Act 1974* (Cth) ss 77 and 151BY.
- 82 Modelled on s 10(2) of the *Equal Opportunity for Women in the Workplace Act 1999* (Cth).
- 83 Department of Treasury and Finance, *Victorian Guide to Regulation* (2nd ed, 2007) 3–7.

Promoting Responsible Use of Surveillance in Public Places

5.101 The vast majority of submissions and consultations supported this suggestion.⁸⁴ The Privacy Commissioner herself said:

While I have no settled view as to who should perform this independent regulatory role, a number of the proposed functions are similar to those currently bestowed on the Victorian Privacy Commissioner by the IPA, which include some regulation of surveillance when undertaken by Victorian public sector agencies or contracted service providers. It may therefore make sense, in the absence of a new, specialist, independent regulator, for the functions to be added to these. In addition, in other jurisdictions, privacy or data protection commissioners have regulation of surveillance included in their functions,⁸⁵ to varying extents.⁸⁶

5.102 The Privacy Commissioner also noted, however, that

additional functions will require substantial resources. The extension of the functions of an existing regulator should not be seen as a 'cost neutral' option, otherwise neither the proposed surveillance related functions nor the existing privacy functions will be adequately fulfilled.⁸⁷

5.103 The Victorian Privacy Commissioner currently has a regulatory role in relation to the privacy of personal information held by Victorian government agencies. There is often a close relationship between the use of surveillance and the personal information gathered by those practices. The commission believes that the Privacy Commissioner is the most appropriate body to exercise regulatory functions concerning the use of public place surveillance.⁸⁸

5.104 The Privacy Commissioner has an existing role in relation to some information captured by the use of surveillance in public places. For example, the Commissioner's existing oversight functions extend to surveillance-captured information held by Victorian agencies where that information constitutes 'personal information' for the purposes of privacy legislation.⁸⁹ These functions include educative, examination and monitoring responsibilities.⁹⁰ The Commissioner is also empowered to receive and resolve complaints about the handling of personal information by a public sector agency (including that captured by a surveillance regulator), to issue compliance notices, and to carry out investigations for these purposes.⁹¹

5.105 While the Commissioner is currently empowered to deal with complaints about public agencies only, her educative function is not limited to public agencies.⁹² The commission is of the view that it is a natural extension of the Commissioner's existing functions to regulate the use of surveillance in public places.

RELATIONSHIP WITH OTHER SURVEILLANCE REGULATORS

5.106 As well as the Victorian and federal Privacy Commissioners, there are a number of other regulators with responsibility for some limited aspects of public place surveillance. These include

- the Commissioner for Law Enforcement and Data Security, in relation to Victoria Police's handling of surveillance-captured data in its possession⁹³
- the Director of Liquor Licensing, in relation to the procedures concerning use of security cameras and retention and storage of footage by some licensed venues⁹⁴

- the Victorian Commission for Gambling Regulation, in relation to the collection, storage and retention of security footage by Crown Casino⁹⁵
- the Special Investigations Monitor, in relation to compliance with the SDA by the four Victorian agencies authorised to apply for surveillance device warrants under the Act—Victoria Police, the Office of Police Integrity, The Department of Primary Industries, and the Department of Sustainability and Environment.⁹⁶

5.107 The new regulator should liaise with these agencies about their functions to ensure that the regulatory regimes are consistent, and that particular users are not unnecessarily burdened by obligations under more than one regime.

RECOMMENDATION

9. The functions of the regulator should be exercised by the Victorian Privacy Commissioner.

REVIEW OF VICTORIA POLICE SURVEILLANCE PRACTICES

- 5.108 Victoria Police, Victoria's major law enforcement body, has access to state-of-the-art surveillance technology. Its use of surveillance devices is extensive. We consulted a number of organisations that provided insight into police use of surveillance, including numerous departments and officers within Victoria Police, as well as oversight bodies, including the Commissioner for Law Enforcement Data Security, the Office of Police Integrity, the Special Investigations Monitor and the Supreme Court.
- 5.109 Although the benefits of police use of surveillance are significant—importantly, preventing and solving crime on behalf of the community—the consequences for a person subject to surveillance can also be profound. These include the potential loss of personal liberty following an arrest or conviction.⁹⁷
- 5.110 The commission believes that regulation of police use of surveillance is best achieved through an entirely separate regime from the one we have proposed for general users of surveillance. Surveillance is only one of the many powers of investigation and crime prevention available to police, and the commission's view is that to consider police use of surveillance in isolation from the broader contexts would be to consider only part of the picture. Appropriately, police use of surveillance is currently regulated by a separate regime from that of other bodies. Regulation includes the warrant-based process under the SDA, and provisions in other state and Commonwealth laws. Therefore, although police officers are subject to sanctions that do not apply to other surveillance users, they also engage in activities, with judicial authorisation, that are otherwise prohibited.
- 5.111 Victoria Police routinely use a variety of surveillance technologies, for example, video surveillance, including stationary CCTV systems, hand-held devices and cameras fitted in vehicles. In some instances, this is coupled with things such as automatic number plate recognition (ANPR) software, which may determine the registered owner of a vehicle from a photograph of the vehicle's numberplate. The Victorian Government has also announced its intention to provide funding for police use of facial recognition software, to be used in conjunction with CCTV to identify individuals from their images.⁹⁸

- 84 Submissions 5, 9, 12, 29; Consultations 5, 9, 14, 27, 28.
- 85 Including the Netherlands, the UK, Ireland, Canada, New Zealand, Germany, Norway, Greece.
- 86 Submission 29.
- 87 Submission 29.
- 88 Surveillance is regulated under information privacy laws in a number of countries, including New Zealand, the UK, Canada, Ireland and The Netherlands. See Victorian Law Reform Commission, *Surveillance in Public Places*, Consultation Paper 7 (2009) [5.15–5.172] for detail.
- 89 This is discussed in detail in Chapter 3.
- 90 *Information Privacy Act 2000* (Vic) ss 58(o),(g), (l), (k).
- 91 *Information Privacy Act 2000* (Vic) pt 5, pt 6, ss 34, 45.
- 92 *Information Privacy Act 2000* (Vic) s 58(a).
- 93 *Commissioner for Law Enforcement Data Security Act 2005* (Vic) ss 4, 11, 12.
- 94 *Liquor Control Reform Act 1998* (Vic) s 18B.
- 95 *Casino Control Act 1991* (Vic) ss 59(2), 122(1)(r).
- 96 *Major Crimes (Special Investigations Monitor) Act 2004* (Vic) ss 4, 11, 12; *Surveillance Devices Act 1999* (Vic) s 30P.
- 97 The leaking of confidential files from the Victoria Police's covert surveillance unit to organised crime figures in 2008 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. See also Office of the Victorian Privacy Commissioner, 'Briefing on the Aquasure Memorandum of Understanding' (Press Release, 10 December 2009).
- 98 Minister for Police and Emergency Services, 'Facial Recognition Technology will Catch Criminals' (Press Release, 30 April 2007).

Promoting Responsible Use of Surveillance in Public Places

- 5.112 In addition to video surveillance, police commonly use listening devices, including handheld devices and those installed at specific locations. Potential suspects may also be tracked, for example, through their mobile phone. Other less common methods of surveillance, such as drug and explosive-detection dogs, are also used. Police must obtain a warrant issued by a judge to conduct intrusive covert surveillance.⁹⁹
- 5.113 There is also a growing trend for police to use data provided by other Victorian bodies, including government departments, local councils, private organisations and individuals. In some cases this is provided on an adhoc basis, in others, there are formal agreements in place. The collection and subsequent use of these data frequently falls outside the regulatory regime designed to deal with police use of surveillance.
- 5.114 It is important that regulation of police use of surveillance data responds to the rapidly increasing sophistication of surveillance technologies and the increasing variety of methods to obtain data. The SDA (the primary Act relating to law enforcement use of surveillance in Victoria) is over a decade old and no longer adequately covers all surveillance technologies or surveillance-captured data accessed by police. For this reason, it is the commission's view that there should be a review of both police use of public place surveillance technologies and the data acquired by its use. Victoria Police, like other users of public place surveillance, should have the benefit of appropriate 'best practice' guidelines. Such guidelines should take into account the principles proposed by the commission to regulate general surveillance use.
- 5.115 There are a number of specialist bodies that have an oversight role in relation to Victoria Police and, importantly, access to its data. The Commissioner for Law Enforcement Data Security (CLEDS) is the most appropriate body to undertake a review of the use of surveillance by Victoria Police.
- 5.116 The CLEDS's primary role is to 'promote the use by Victoria Police of appropriate and secure management practices for law enforcement data'.¹⁰⁰ All data, including 'any information obtained, received or held' by Victoria Police, fall within the Commissioner's jurisdiction,¹⁰¹ and, importantly, this includes data obtained through the surveillance activities of other bodies. The powers of the Commissioner include the capacity to establish standards, monitor compliance with those standards, and to conduct periodic reviews of 'any matter related to law enforcement data security'.¹⁰²
- 5.117 The commission is of the view that the CLEDS should conduct a review of, and create guidelines for, Victoria Police's use of surveillance and surveillance-captured data. Consideration may need to be given to whether current CLEDS powers are sufficient for the Commissioner to comprehensively carry out these functions.

RECOMMENDATION

10. The Commissioner for Law Enforcement and Data Security should conduct a review of, and create guidelines for, Victoria Police's use of surveillance and surveillance-captured data.

REGULATORY FEATURES NOT RECOMMENDED AT THIS STAGE

REGISTRATION OR LICENSING OF SOME SURVEILLANCE USERS

- 5.118 In our Consultation Paper we canvassed the options of requiring users of surveillance to register their use with a regulator, or to apply for a licence for their use of specific public place surveillance devices. Many European countries require some users of public place surveillance to register with a regulator,¹⁰³ or to obtain a licence for their surveillance use.¹⁰⁴
- 5.119 There was a mixed response to these proposals. A number of submissions supported a registration scheme, mainly because such a scheme would provide the regulator with knowledge of surveillance users in Victoria.¹⁰⁵ Other submissions raised concerns about the introduction of such a scheme. It was noted that such a scheme could lead to the potential for data to be shared more readily between organisations and agencies.¹⁰⁶ Some stakeholders (including Victoria Police) questioned the practicability of a registration scheme and noted the potential for it to be very resource intensive.¹⁰⁷ It was suggested that the benefits of such a scheme should be carefully weighed up against the potential costs.¹⁰⁸
- 5.120 The response to the proposal of a licensing scheme for users of some forms of surveillance was also mixed. A number of submissions supported licensing for surveillance practices described variously as those that are 'invasive',¹⁰⁹ 'intrusive',¹¹⁰ that 'have a significant impact on privacy'¹¹¹ or are used in 'particularly sensitive situations/areas'.¹¹² On the other hand, many submissions commented on the cost or resource requirements of establishing and maintaining a licensing system.¹¹³ The Victorian Privacy Commissioner was 'sceptical of the efficacy of a licensing regime', and preferred the prohibition of some forms of invasive or potentially offensive surveillance.¹¹⁴
- 5.121 The commission believes that requiring significant surveillance users to provide regular advice about their surveillance use is a better way for the regulator to acquire information than a registration scheme. The introduction of our proposed scheme would render registration unnecessary. The commission does not think the potential benefits of requiring organisations to register their surveillance use with a regulator outweigh the potential regulatory burden of having to register, nor the resulting resource burden on the regulator.
- 5.122 The commission is also of the view that our proposed scheme is a more appropriate method of regulating particularly invasive forms of surveillance than a licensing scheme. An example of a particularly invasive form of surveillance is the body scanners trialled at some Australian airports in 2009.¹¹⁵ Although the federal government has recently announced its intention to introduce these at some international airports,¹¹⁶ the devices are currently expensive and resource intensive to use; the commission is not aware of plans for their use by any Victorian bodies in the near future. The commission proposes that all users of particularly invasive surveillance devices be required to provide advice to the regulator, and to ensure they are conducting their surveillance in accordance with the proposed surveillance principles. When the use of such devices becomes widespread in Victoria, the regulator may wish to recommend a licensing scheme (or other appropriate method of regulation) for the users of such devices.

99 Law enforcement use of surveillance is described in more detail in Chapter 2.

100 Commissioner for Law Enforcement Data Security, *About CLEDS (2009)* <www.cleds.vic.gov.au/content.asp?Document_ID=10470> at 16 December 2009.

101 *Commissioner for Law Enforcement Data Security Act 2005 (Vic)* s 3.

102 Commissioner for Law Enforcement Data Security, above n 100.

103 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.

104 Including Norway, Germany and Sweden. See Victorian Law Reform Commission, above n 88, 150 for detail.

105 Submissions 5, 14, 29, 31, 33, 34, 40, 42.

106 Submission 34.

107 Submissions 11, 21.

108 Submission 21.

109 Submission 38.

110 Consultation 4.

111 Submission 34.

112 Submission 39.

113 Submission 13.

114 Submission 29. The Commissioner noted that in the absence of a warrant, prohibition should include, at a minimum, covert surveillance, x-ray body scanners, infrared equipment and other equipment operating outside the visible light spectrum.

115 Discussed in Chapter 2.

116 Anthony Albanese MP, Minister for Infrastructure, Transport, Regional Development and Local Government, 'Strengthening Aviation Security' (Press Release, 9 February 2010).

Promoting Responsible Use of Surveillance in Public Places

A COMPLAINT-HANDLING POWER FOR THE REGULATOR

- 5.123 Some submissions suggested that the regulator should receive and investigate complaints made by members of the public about misuse of public place surveillance.¹¹⁷ The proposed regime is a more appropriate model for regulating public place surveillance than a complaints-based regime, as it is designed to deal primarily with systemic issues rather than individual grievances.
- 5.124 There are already some processes in place to deal with individual complaints arising from some aspects of misuse of public place surveillance. Existing federal and Victorian privacy laws, for example, have a mechanism for dealing with complaints relating to misuse of personal information, including that captured by way of a surveillance device.¹¹⁸ Additionally, the proposed statutory causes of action discussed in Chapter 7 will allow an individual response to serious invasions of privacy. These mechanisms should provide adequate redress for individuals harmed by misuse of a surveillance device.
- 5.125 The commission's proposed model places the onus on users to demonstrate their compliance with laws and best practice guidelines, rather than on individuals to notify the regulator of misuse. This is particularly appropriate in the public place surveillance context, as in many instances it is likely that people will be unaware of the fact that they are the victim of misuse of a surveillance device.
- 5.126 There is a noticeable shift away from complaints-based models in regimes designed to protect people's rights. For example, the Victorian Attorney-General noted the shortcomings of a complaints-based model in relation to Victoria's equal opportunity laws in his 2008 *Justice Statement*:
- This rather narrow approach places the onus for change on the willingness of individual victims of discrimination to come forward and take the risks and burden of pursuing a complaint through an unfamiliar legal system.*¹¹⁹
- 5.127 Under the proposed model the regulator may receive notification from the public about suspected inappropriate use of surveillance devices. The regulator will not be obliged to act on this advice in every case. Instead, the regulator may choose to request information from the surveillance user, or examine their surveillance practices, to determine if they are acting in compliance with the law and best practice guidelines.

GENERAL OWN-MOTION INVESTIGATORY POWERS

- 5.128 The commission recommends that the regulator have limited investigatory powers in relation to the most serious instances of inappropriate use of public place surveillance. In some cases, such investigations may lead to civil penalty proceedings.
- 5.129 In our Consultation Paper we suggested the regulator could be given the power to carry out investigations into the public place surveillance practices of particular agencies and organisations. There was a mixed response to this proposal.¹²⁰
- 5.130 The Victorian Privacy Commissioner's current investigative power is limited to her complaint-handling function.¹²¹ The commission is of the view that it is more appropriate that the focus of the surveillance regulator be on educating, providing advice and working collaboratively with surveillance users to encourage them to employ best practice. If, later, the regulator believes that the educative role is not sufficient, and that investigatory powers are needed, the government can be advised of this in a report to parliament.

PROCUREMENT STANDARDS AS A TOOL TO ENCOURAGE COMPLIANCE

- 5.131 In our Consultation Paper we raised the possibility of making compliance with a voluntary public place surveillance standard a condition of entering into a contractual agreement with the Victorian Government. Although some organisations supported the proposal of linking voluntary standards to government procurement criteria,¹²² it was also noted this strategy may have limited effect for a number of reasons, including that only a small proportion of businesses compete for contracts with government through the tender process, and that the government sector makes up a large proportion of surveillance users.¹²³
- 5.132 The commission is of the view that requiring all government agencies and larger private users of public place surveillance to provide advice to a regulator about their compliance with best practice standards is a more effective way of ensuring that the major users are conducting public place surveillance responsibly. Many of the organisations who provide goods and services to the Victorian Government will be covered by these requirements; it is unnecessary to burden them with further requirements.

CONCLUSION

- 5.133 This chapter outlines the first and second limbs of the commission's proposed regulatory model for regulating public place surveillance in Victoria. These are based on the approach to regulation outlined in Chapter 4—a flexible, principle-based approach that is primarily educative and focuses on achieving best practice.
- 5.134 In devising our principles and the functions of a proposed surveillance regulator, the commission has been guided by its extensive consultations, site visits and submissions. It has also been informed by the Charter framework for balancing the competing rights and interests that arise in relation to public place surveillance.
- 5.135 The second limb of the commission's regulatory approach—the creation of an independent regulator—is designed to provide surveillance users with practical advice on how to apply the principles to their use of surveillance. The focus of the regulator is to encourage users to conduct surveillance responsibly, and to inform the public about their rights and responsibilities.
- 5.136 Regulatory options for dealing with particularly offensive or privacy-invasive forms of surveillance are outlined in the following chapters.

117 Submissions 5, 12, 42.

118 Discussed in Chapter 3.

119 Department of Justice [Victoria], *Attorney-General's Justice Statement 2: The Next Chapter* (2008) 22.

120 Supporters of the proposal included Submissions 5, 12, 36, 40; Consultations 5, 9, 28. Other submissions did not support the proposal, or did not canvass the issue.

121 See *Information Privacy Act 2000* (Vic) ss 34 and 58(i).

122 Submissions 4, 5, 7, 26, 35, 37, 40; Consultation 27.

123 Submissions 14, 29, 33.

Chapter 6

Modernising the Surveillance Devices Act

CONTENTS

- 108 Introduction
- 108 Background
- 108 Definitions
- 112 Prohibition of surveillance devices in toilets
- 112 Regulating tracking devices
- 117 Removing the participant monitoring exception
- 121 A civil penalty regime
- 122 A new offence for improper use of a surveillance device
- 125 Conclusion

Modernising the Surveillance Devices Act

INTRODUCTION

- 6.1 This chapter deals with those parts of the *Surveillance Devices Act 1999* (Vic) (SDA) where the commission recommends change to deal with advances in technology and to modernise the way we regulate the use of surveillance devices.

BACKGROUND

- 6.2 The Victorian parliament first dealt with surveillance devices in 1969 when it introduced the *Listening Devices Act 1969* (Vic), which prohibited the use of listening devices to record or monitor private conversations. That Act also included requirements for obtaining a warrant to undertake covert surveillance with a listening device and provided exemptions for police in specific circumstances.
- 6.3 In 1999 parliament responded to advances in technology and the more widespread use of surveillance by passing the SDA. This Act regulates the use of optical surveillance devices, tracking devices and data surveillance devices as well as listening devices. The SDA has been amended on a number of occasions since then. Major amendments include prohibiting surveillance of workers in toilets and change rooms,¹ and establishing an oversight and monitoring role for the Special Investigations Monitor in relation to law enforcement use of surveillance.²
- 6.4 Surveillance technology has become increasingly sophisticated, affordable, concealable and unobtrusive. Its use is now commonplace. People are subject to surveillance every day when they use public transport, shop for groceries, attend sporting events and walk down city streets.³
- 6.5 Technology has also changed the way people use public places. Activities that many people would still consider private, such as personal telephone conversations, now regularly take place in public places on mobile phones.
- 6.6 To reflect these changes in behaviour, and to ensure that the law keeps pace with advances in technology, the commission recommends a number of changes to clarify, modernise and strengthen the SDA. These include amending some important definitions to reflect contemporary uses of surveillance devices, expressly prohibiting surveillance in toilets and change rooms, strengthening the prohibition on participant monitoring, introducing a new offence to prohibit particularly offensive uses of surveillance devices, and introducing a civil enforcement regime into the Act.

DEFINITIONS

PRIVATE ACTIVITY

- 6.7 The SDA prohibits a person from using a listening device to monitor⁴ a 'private conversation' to which they are not a party if not all the people in the conversation have given their consent.⁵ Similarly, the Act prohibits a person from using an optical surveillance device to monitor a 'private activity' to which they are not a party if not all the people conducting the activity have given their consent.⁶
- 6.8 Under the Act, a conversation or activity is 'private' if it occurs in circumstances that reasonably indicate the parties desire it to be heard or observed by themselves only, and when they may reasonably expect that they will not be heard or observed by someone else.⁷

- 6.9 Currently, the definitions of ‘private conversation’ and ‘private activity’ differ in relation to the physical location of the conversation or activity being monitored. Although an activity cannot be ‘private’ if it occurs outside a building, a conversation may be ‘private’ regardless of where it occurs. It is unlawful for a person to use a listening device to record a private conversation without consent, either indoors or outdoors.⁸ By contrast, although a person cannot use an optical surveillance device indoors to record a private activity without consent, there is no such prohibition on the use of an optical surveillance device outdoors. Consequently, the SDA offers no protection against highly intrusive visual surveillance in outdoor places.⁹
- 6.10 During the parliamentary debates that accompanied the passage of the SDA a number of members referred to the lack of protection for private activities in outdoor places, such as beaches and backyards.¹⁰ This issue generates community interest from time to time, such as when the satellite images and photographs published by Google Street View, and used by some NSW and Victorian councils, attracted publicity.¹¹
- 6.11 Advances in technology have meant that these different provisions in the SDA for listening devices and optical surveillance devices produce illogical outcomes. For example, the prohibition on recording a private conversation that occurs outside a building without consent may be lawfully circumvented by the use of a video recorder used in conjunction with lip-reading technology or services. Further, using a video recorder with sound recording capacity to record a private occurrence outside a building could breach the listening device offence in section 6 of the SDA without breaching the optical surveillance device offence in section 7. This is because of the limited definition of ‘private activity’ in the SDA.
- 6.12 Surveillance device legislation in Western Australia and the Northern Territory prohibits (with exceptions) the use of an optical surveillance device to record a private activity.¹² Neither jurisdiction makes a distinction between whether the activity occurs indoors or outdoors.¹³ As well as this, NSW legislation that regulates optical surveillance devices does not make a distinction between indoor and outdoor activities.¹⁴
- 6.13 The commission believes the SDA should prohibit the use of an optical surveillance device to monitor private activities that occur outdoors as well as indoors. This change would ensure consistency in the regulation of surveillance devices and would bring Victorian surveillance device legislation in line with legislation in other Australian jurisdictions.
- 6.14 Most visual surveillance activities that occur outdoors would not be affected by the commission’s proposal. This is because the prohibition in section 7 of the SDA against the use of a visual surveillance device applies only to ‘private activities’. These are activities that people do not wish others to observe, and which are not carried out in circumstances where they ought to reasonably expect that someone else may observe it. There are, however, some ‘private activities’ that do occur outdoors and in public places. It should be unlawful for people to monitor these activities with a visual surveillance device.

- 1 *Surveillance Devices Act 1999* (Vic) s 9B. This was in response to our recommendation: Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005) rec 30.
- 2 *Surveillance Devices Act 1999* (Vic) ss 30P, 30Q.
- 3 The use of surveillance in Victoria is detailed in Chapter 2.
- 4 The word ‘monitor’ is used here in a generic sense. Section 6 of the Act makes it unlawful to use a listening device ‘to overhear, record, monitor or listen to a private conversation’. *Surveillance Devices Act 1999* (Vic) s 6.
- 5 *Surveillance Devices Act 1999* (Vic) s 6.
- 6 *Surveillance Devices Act 1999* (Vic) s 7.
- 7 The terms ‘private activity’ and ‘private conversation’ are defined in section 3 of the *Surveillance Devices Act 1999* (Vic).
- 8 *Surveillance Devices Act 1999* (Vic) s 6.
- 9 *Surveillance Devices Act 1999* (Vic) s 7.
- 10 Victoria, *Parliamentary Debates*, Legislative Council, 11 May 1999, 524–5 (Maree Luckins); Victoria, *Parliamentary Debates*, Legislative Assembly, 22 April 1999, 551 (Robert Hulls), 555 (Victor Pertou), 559 (Hurtle Lupton).
- 11 Roundtable 10; Asher Moses and Dewi Cooke, ‘Anyone for a Gentle Google Down Wisteria Lane?’, *The Age* (Melbourne), 6 August 2008, 5. See discussion in Chapter 2.
- 12 *Surveillance Devices Act 1998* (WA) s 6; *Surveillance Devices Act 2007* (NT) s 12.
- 13 *Surveillance Devices Act 1998* (WA) s 3; *Surveillance Devices Act 2007* (NT) s 4.
- 14 *Surveillance Devices Act 2007* (NSW) s 8. Note that there are some exceptions to the prohibition, including for law enforcement purposes.

Modernising the Surveillance Devices Act

RECOMMENDATION

11. The words ‘an activity carried on outside a building’ should be removed from the definition of ‘private activity’ in section 3 of the SDA so that it reads:

private activity means an activity carried on in circumstances that may reasonably be taken to indicate that the parties to it desire it to be observed only by themselves, but does not include an activity carried on in any circumstances in which the parties to it ought reasonably to expect that it may be observed by someone else.

IMPLIED CONSENT

- 6.15 The prohibitions in the SDA concerning the use of listening, optical, tracking or data surveillance devices do not apply if the surveillance user has the express or implied consent of the person being monitored.¹⁵ As the Act does not define ‘consent’ common law principles concerning the meaning of consent probably apply. For example, at common law, a person must have capacity for consent to be valid and that consent must be given freely and voluntarily.¹⁶
- 6.16 The notion of consent—particularly implied consent—is sometimes difficult to characterise when dealing with many common surveillance practices in public places. If, for example, a retail outlet has a sign on the door stating that cameras are in use on the premises, does this mean that all customers give their implied consent to being filmed when they walk into the shop, including when they enter change rooms to try on clothing? Does this include people who might not have the capacity to give consent, or those who cannot read the sign? In some circumstances it may be inconvenient (or impossible) for a person to opt out of being subject to surveillance, and therefore any implied consent may not be truly voluntary.
- 6.17 In its Privacy Report the Australian Law Reform Commission (ALRC) discussed the difficulties raised by the concept of consent, noting, in relation to personal information:
- 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 or disclosed.*¹⁷
- 6.18 To address this, the ALRC recommended that the Office of the Privacy Commissioner ‘develop and publish further guidance about what is required of agencies and organisations to obtain an individual’s consent for the purposes of the Privacy Act’.¹⁸ In our Consultation Paper we asked stakeholders whether a regulator should develop guidelines to clarify the meaning of consent. Many submissions supported this proposition. However, of those that did not, Victoria Police said this was a matter for parliament and the judiciary,¹⁹ and the Victorian Privacy Commissioner said the meaning of consent should be defined in the SDA itself.²⁰
- 6.19 Submissions also noted the difficulties in defining ‘implied behaviour’. The St Kilda Legal Service noted that consent should not be implied when an individual has no reasonable choice about being in a particular place. The service noted that the most marginalised groups—for example, homeless people—have little choice in avoiding public place surveillance.²¹ The Victorian Privacy Commissioner noted that even implied consent should be free, revocable and fully informed.²²

- 6.20 From a commercial perspective Sensis (the information and advertising arm of Telstra) said the lawfulness of their location-based services relied on implied consent. When, for example, a mobile phone user is offered details of the location of the closest petrol station via text message, the service provider must identify the phone owner's location in order to provide that information. By requesting the service has the phone owner consented to having their location tracked by the service provider? Sensis said the status quo, where implied consent is not defined, operates effectively and flexibly and does not require legislative amendment.²³
- 6.21 The commission acknowledges that in many instances it makes little sense to suggest that people whose activities are monitored by surveillance equipment in public places have given actual consent to a 'private activity' or a 'private conversation' being monitored by an optical surveillance device or a listening device. Nevertheless, the notion of 'implied consent'²⁴ remains the most practical dividing line between behaviour that should be prohibited in a public place because it is highly intrusive, unannounced and undetectable, and behaviour that should be permitted because reasonable attempts have been made to alert members of the public to the fact that some form of intrusive surveillance is occurring.
- 6.22 Given the widespread use of surveillance devices in public places, it is important to encourage surveillance device users to give adequate notice of their activities when they engage in practices that may involve monitoring of a 'private conversation' or a 'private activity'. The SDA should actively encourage the practice of giving adequate notice of surveillance, by signage or other means, in these circumstances. The SDA should be amended to direct courts, when deciding whether a person has given implied consent to conduct that would otherwise fall within sections 6–9 and 11–12 of the SDA, to consider whether the defendant should have given adequate notice of the surveillance activities and whether in fact that notice was given. Although common law principles concerning the meaning of implied consent would otherwise continue to apply, this change would encourage surveillance users to ensure they do not conduct highly intrusive public place surveillance without providing adequate notice of their activities.
- 6.23 In some instances it may be appropriate to make limited use of well-placed signs, perhaps containing an image of a camera, to give people adequate notice of the fact that a CCTV surveillance system is being used in a way that is particularly intrusive. The regulator will be well placed to advise people about how to strike a balance between reasonable notice, the cost of erecting signs and the unsightly impact of some notices.

- 15 *Surveillance Devices Act 1999* (Vic) ss 6–9.
- 16 Jeremy Douglas-Stewart, *Annotated National Privacy Principles* (2007), cited in Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1, Final Report* 108 (2008) [19.9].
- 17 Australian Law Reform Commission, *For Your Information* above n 16 [19.59].
- 18 *Ibid* rec 19–1.
- 19 Submission 11.
- 20 Submission 29.
- 21 Submission 14.
- 22 Submission 29.
- 23 Submission 19.
- 24 We use the term 'implied consent' to mean behaviour by a person, falling short of express agreement, which would cause a reasonable observer to conclude that the person has agreed to a particular course of conduct.

RECOMMENDATION

12. The SDA should be amended so that courts are directed to consider whether a public place surveillance user has given adequate notice of their surveillance activities when considering whether a person has given 'implied consent' to any of the conduct that falls within sections 6–9 and 11–12 of the SDA.

Modernising the Surveillance Devices Act

PROHIBITION OF SURVEILLANCE DEVICES IN TOILETS

- 6.24 At present, the SDA prohibits use of an optical surveillance device to monitor ‘private activity’—defined in the Act as an activity 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.²⁵
- 6.25 There is, however, uncertainty about the reach of this prohibition because in some instances a person would reasonably expect to be seen by others when using communal facilities, such as in open showers and at urinals.²⁶ Perhaps because of the uncertainty about the reach of the current law, some fitness centres have independently instituted policies to ban mobile telephones (which may have camera devices) in such areas.²⁷ The Victorian Privacy Commissioner has queried whether the comment in the explanatory memorandum to the SDA 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.*²⁸
- 6.26 The commission is of the view that the SDA should be amended 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, this prohibition would not apply to law enforcement officers acting under warrant.
- 6.27 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. This view was strongly expressed in submissions and consultations.²⁹ Further, many international codes of practice and guidelines³⁰ prohibit, or greatly restrict,³¹ surveillance in such areas.
- 6.28 This reform proposal reflects 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 bathrooms.³² The Victorian parliament adopted that proposal in 2006 by inserting section 9B into the SDA.

RECOMMENDATION

13. The SDA should be amended to expressly prohibit the use of an optical surveillance device or listening device to observe, listen to, record or monitor any activity in toilets, shower areas and change rooms which form a part of any public place. This prohibition should include a law enforcement exemption similar to that in section 9B(2) of the SDA.

REGULATING TRACKING DEVICES

- 6.29 The use of tracking devices is regulated far more strictly under the SDA than the use of optical surveillance or listening devices. It is unlawful to use a tracking device without the consent of the person being tracked, unless one of the law enforcement exceptions applies. In contrast, it is unlawful to use an optical surveillance or listening device only when monitoring a *private activity* or a *private conversation* without consent. Again, this is subject to the law enforcement exceptions.

6.30 This distinction reflects the serious privacy implications of tracking a person without their consent. These implications were discussed by the New Zealand Law Commission (NZLC), which recommended that tracking a person without their consent should be generally prohibited in New Zealand. The NZLC notes:

*Covert tracking robs people of the ability to choose whether or not others know where they are at a particular time. It can reveal very private information: that a person visited an abortion clinic or a gay bar for example ... In the most serious cases, being tracked may make people feel insecure, or may genuinely threaten their safety if it is done by a violent ex-partner, for example.*³³

6.31 Currently, not all tracking devices are regulated under the SDA. Although an optical or listening device is defined as 'any device capable' of being used to record a person's voice or activity under the Act, a tracking device is defined as a device the *primary purpose* of which is to determine the geographical location of a person or an object.³⁴ This means that a device that is capable of tracking, but is not primarily used for that purpose (such as a mobile phone with GPS capacity), is not a tracking device covered by the Act.

6.32 In our Consultation Paper we asked whether it was appropriate for the definition of 'tracking device' to be amended so it includes any electronic device capable of being used to determine the geographical location of a person or object. This change would mean that the definition of 'tracking device' is consistent with the definitions of other surveillance devices that are concerned with the capacity of a device rather than its primary purpose.

6.33 There was broad support for amending the definition of 'tracking device' in this way. Consultees raised concerns about the unregulated use of some tracking devices. For example, the Victorian Women's Legal Service expressed concern about 'stalkers' using tracking devices with no protection for the person who is being stalked.³⁵

6.34 Amending the definition of 'tracking device' would create consistency with NSW legislation. The *Surveillance Devices Act 2007* (NSW) does not use the 'primary purpose' test. It defines a 'tracking device' as 'any electronic device capable of being used to determine or monitor the geographical location of a person or an object' (emphasis added).

6.35 The commission recommends that the definition of 'tracking device' in the SDA be amended so that it includes all electronic devices capable of being used to determine the geographical location of a person or object. However, we also recognise that there are many legitimate and beneficial uses of tracking devices. The SDA currently includes the following exemptions:

- the installation, use or maintenance of a tracking device in accordance with a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation
- the installation, use or maintenance of a tracking device in accordance with a detention order or supervision order or an interim order under the *Serious Sex Offenders (Detention and Supervision) Act 2009* (Vic)
- the installation, use or maintenance of a tracking device in accordance with a law of the Commonwealth.³⁶

25 Explanatory Memorandum, Surveillance Devices Bill 1999 (Vic) cl 3.

26 Office of the Victorian Privacy Commissioner, *Mobile Phones with Cameras*, Info Sheet 05.03 (2003) 4.

27 'Tighter Rules on Camera Phones', *Herald Sun* (Melbourne), 1 July 2004, 1.

28 Office of the Victorian Privacy Commissioner, above n 26, 4.

29 Submissions 2, 4, 5, 9, 13, 29, 33, 34, 37, 38, 40; Roundtables 2, 8, 9, 10, 12, 13, 14, 15, 20, 21, 24, 25, 26, 27.

30 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* (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 4 March 2009.

31 See eg, Information Commissioner's Office [UK], above n 30, 9.

32 Victorian Law Reform Commission, *Workplace Privacy*, above n 1 rec 30.

33 New Zealand Law Commission, *Invasion of Privacy: Penalties and Remedies*, Report No 113 (2010) [3.51].

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

35 Submission 36.

36 *Surveillance Devices Act 1999* (Vic) s 8(2).

Modernising the Surveillance Devices Act

- 6.36 The commission is of the view that these are appropriate and necessary exemptions, and should continue to apply. In addition, there are other legitimate uses of tracking devices that should be exempted from the general prohibition against the use of a tracking device without consent. These are discussed below.

AUTOMATIC NUMBER PLATE RECOGNITION

- 6.37 Automatic number plate recognition (ANPR) devices use pattern recognition software to automatically detect and read the licence plates of vehicles that pass the system's cameras and match these against registration records on a database. ANPR identifies the time and date of the scan and the GPS location. When multiple ANPR devices are used together, they can track the movement of a vehicle.
- 6.38 ANPR technology is a classic example of 'convergence'³⁷ of surveillance technologies, as it uses both optical surveillance (cameras) and tracking devices (GPS) in order to determine the location of a vehicle. The use of ANPR does not infringe the prohibition on the use of optical surveillance devices in the SDA, as optical surveillance is prohibited in relation to a private activity only. However, as the current and proposed prohibition on the use of tracking devices is not limited to 'private activities', the continued use of ANPR is relevant when considering the regulation of tracking devices.
- 6.39 A number of organisations in Victoria use ANPR technology. For example, in 2009 Victoria Police trialled the use of ANPR in police cars to record the details of passing vehicles and detect those that may be unregistered or stolen.³⁸ It is also possible for police to search for persons of interest using this technology. ANPR is also used to assist in the collection of road tolls on private tollways in Melbourne,³⁹ and VicRoads uses the technology with red-light and speeding cameras across Victoria. In addition, ANPR may be used by governments and private organisations for a number of applications, including controlling access to restricted areas, congestion taxes, monitoring freight movement and calculating fees for unattended car parks.⁴⁰
- 6.40 Government agencies in many countries use ANPR technology for road safety and law enforcement purposes.⁴¹ It is estimated that there are at least 10 000 ANPR cameras in operation in the UK. These cameras provide data about over 10 million number plates per day to a national database run on behalf of the Association of Chief Police Officers. The data are kept for two years and are used for a number of purposes, including evidence in criminal trials. Concerns have been raised about possible misuse of this information.⁴²
- 6.41 In its submission to the commission Victoria Police noted that the commission's proposed changes to the definition of tracking device would have a significant impact on police operations, particularly their use of ANPR technology, which they believe does not currently fall within section 8 of the SDA. Victoria Police believes that it would be 'administratively unworkable' to require police to obtain a warrant each time they wish to use ANPR. Victoria Police also raised concerns about the impact on emergency services in the case of missing persons.⁴³ In addition, it seems desirable that VicRoads and tollway operators be permitted to continue to use ANPR for road safety and tolling purposes.
- 6.42 In NSW, ANPR has been an integral part of the Safe-T-Cam traffic monitoring system since 1989.⁴⁴ In addition, NSW Police trialled ANPR use in 2009.⁴⁵ It appears that these activities fall outside of the general prohibition against the use of tracking devices in section 9 of the *Surveillance Devices Act 2007* (NSW) because of the exception in section 9(2)(c) that extends to 'the installation, use or maintenance of a tracking device for a lawful purpose'.

- 6.43 This exception to the prohibition against using a tracking device without consent is both vague and unnecessarily broad. There are better ways of ensuring that all relevant interests are taken into account when deciding whether technology of this nature should be used to track the movements of people who are acting lawfully, as well as those who are acting unlawfully. One way would be to allow specific law enforcement activities to be exempted by regulation from the general prohibition against using a tracking device without consent.
- 6.44 This process should ensure that there is appropriate oversight of any decision to provide a law enforcement exception to the general prohibition against using a tracking device without consent. It is highly likely that the government would seek advice from the Privacy Commissioner and the proposed new surveillance regulator before preparing a regulation. Any regulation would be subject to parliamentary scrutiny and disallowance under the relevant provisions of the *Subordinate Legislation Act 1994* (Vic).
- 6.45 The use of ANPR technology should be carefully monitored because of its potential for capturing vast amounts of information about individuals who are behaving lawfully. ANPR was the subject of a study by the Queensland Parliamentary Travelsafe Committee, which released a report in September 2008. A number of submissions (including those by the federal and Victorian Privacy Commissioners) raised privacy concerns in relation to the technology, including the appropriateness of recording and retaining data of people not identified as having done something illegal, and the potential for ANPR to be used for unintended purposes, referred to as ‘function creep’.⁴⁶
- 6.46 The Committee made a number of recommendations, including the installation of signs that inform motorists that their image may be recorded, and legislation that contains safeguards and controls governing the use of ANPR technology. The Queensland government has implemented a number of the recommendations, including amending signs, and has committed to consider the Committee’s other recommendations concerning legislation.⁴⁷
- 6.47 The commission recommends that the proposed regulator should advise parliament regularly about the use of ANPR technology in Victoria, including whether the current regulatory controls are adequate.

MANAGEMENT AND CARE OF PATIENTS

- 6.48 Another issue that arises in relation to tracking devices is their use in the management and care of people suffering from dementia and other memory-affecting conditions. Alzheimer’s Australia recommends that carers consider the use of a GPS-enabled tracking device, such as a bracelet-type device, to monitor a person with dementia so that the individual can freely go for walks on their own but can be easily located if they are lost or disoriented.⁴⁸ In many instances the person being tracked may not have the capacity to consent to being monitored by a device that enables them to be located.
- 6.49 It should be possible to use tracking devices to protect the health, safety and wellbeing of people in these circumstances. The New Zealand Law Commission has considered this issue in relation to its proposal that new surveillance legislation include a prohibition on the use of tracking devices. The Commission notes:

*We think that it should be a defence to the tracking device offence that the use of the tracking device was necessary for the protection of the health, safety or wellbeing of any person, or for the protection of public health or safety, and was no more extensive than reasonably necessary for those purposes.*⁴⁹

- 37 Convergence is discussed in Chapter 2.
- 38 Michael Daley MP, NSW Minister for Police, ‘New Mobile Technology to Help Capture Unregistered and Stolen Vehicles’ (Press Release, 17 September 2009).
- 39 Site Visit 9.
- 40 Parliamentary Travelsafe Committee, Queensland Parliament, *Inquiry into Automatic Number Plate Recognition Technology*, Report 51 (2007) 2.
- 41 Ibid 4.
- 42 See eg, S A Mathieson, *The ANPR Secret* (2010) Kable <www.kable.co.uk/automatic-numberplate-recognition-police-anpr-gc-feb10> at 3 March 2010.
- 43 Submission 11.
- 44 Parliamentary Travelsafe Committee, above n 40, 5.
- 45 Daley, above n 38.
- 46 Parliamentary Travelsafe Committee, above n 40, 14.
- 47 Queensland Government, *Queensland Government Response to the Parliamentary Select Committee on Travelsafe’s Report No 51: Report on the Inquiry into Automatic Number Plate Recognition Technology* (2009) <www.parliament.qld.gov.au/view/legislativeAssembly/tableOffice/documents/TabledPapers/2009/5309T434.pdf> at 9 March 2010.
- 48 Alzheimer’s Australia, *Update Sheet: Safer Walking for People with Dementia: Approaches and Technologies*, Update Sheet 16 (April 2009) 3.
- 49 New Zealand Law Commission, above n 33, [3.54].

Modernising the Surveillance Devices Act

- 6.50 The Commission notes the defence would cover such situations as
- use of tracking devices to monitor the movements of dementia patients
 - use of tracking devices by parents or guardians to monitor the location of their children
 - use by hospital management to track the movements of patients within the hospital.⁵⁰
- 6.51 These defences may go too far. The family, friends and/or carers of people suffering from dementia and other memory-affecting conditions should be able to use a tracking device to locate that person if they are lost or disorientated. That person's freedom of decision and action is enhanced by permitting them to move around the community as freely as possible so long as they do not pose a threat to their own safety or that of others. If the person is unable to consent to the use of the tracking device because of lack of capacity, there should be an automatic substitute consent-giving regime that is similar to that which applies to consent for medical treatment set out in Part 4A of the *Guardianship and Administration Act 1986* (Vic).
- 6.52 The *Guardianship and Administration Act 1986* (Vic) establishes a hierarchy of people, known as the 'person responsible', who may consent to most forms of medical treatment on behalf of a person who cannot consent to it themselves. These people range from a medical agent and guardian to a spouse or primary carer.⁵¹ This regime should be extended so that the 'person responsible' may consent to the wearing of a tracking device.
- 6.53 The issue of substituted consent for using a tracking device to monitor the location of a child is far more complex. Children of a certain age should be able to move freely around the community without parents tracking them, no matter how well meaning they may be. The proposed new regulator may choose to report to parliament about this issue.

RECOMMENDATION

14. The definition of 'tracking device' in section 3 the SDA should be amended so that it includes all electronic devices capable of being used to determine the geographical location of a person or object.
15. The Governor in Council should be permitted to make regulations that allow specific law enforcement activities to be exempted from the general prohibition in section 8 of the SDA against using a tracking device without consent.
16. The proposed new regulator should advise parliament regularly about the use of ANPR technology in Victoria, including whether the current regulatory controls are adequate.
17. The automatic substitute consent regime in Part 4A of the *Guardianship and Administration Act 1986* (Vic) should be extended so that the 'person responsible' may consent to the installation of a tracking device for a person over the age of 18 years who is incapable of giving consent to the installation of that device.

REMOVING THE PARTICIPANT MONITORING EXCEPTION

- 6.54 The SDA's prohibition on recording a conversation or activity using a surveillance device applies only to people who are not a party to the conversation or activity. It does not prohibit a person from recording a private conversation or activity to which they are a party.⁵² This activity is known as 'participant monitoring'.
- 6.55 At present it is quite lawful for one person to secretly record his or her conversation with another person on a park bench, or to secretly film an encounter with another on a secluded beach. These are places where it might be reasonable for a person to expect that a conversation or activity would not be overheard or seen by others.
- 6.56 Publication of information gained through participant monitoring is unlawful however. Section 11 of the SDA prohibits publication of a record or report of 'private conversation' or 'private activity' that has been made by using a surveillance device.⁵³ There are a number of exceptions to this prohibition that are set out in section 11(2) of the SDA.
- 6.57 It is strongly arguable that it is offensive in most circumstances to record a private conversation or activity to which a person is a party without informing the other participants.⁵⁴ Without this knowledge, those people cannot refuse to be recorded or alter their behaviour. These concerns apply even more strongly in the case of activities or conduct in private places. For example, the SDA currently permits a participant in a sexual act to record that activity without the knowledge and consent of the other party involved.⁵⁵
- 6.58 Finally, as we noted in our Consultation Paper, most Australian states prohibit participant monitoring under their surveillance devices legislation.⁵⁶ Only Queensland and the Northern Territory have similar participant monitoring exceptions to those in the Victorian legislation.⁵⁷

ALLOWING SOME INSTANCES OF PARTICIPANT MONITORING

- 6.59 It is also arguable that some forms of participant monitoring are beneficial and should continue to be permitted. Participant monitoring allows individuals to protect their interests, particularly in 'commercial, business and domestic contexts'.⁵⁸ For example, the commission was told that participant monitoring is used by parties in domestic violence and family law matters, such as when a woman records her ex-husband's conversations with her as evidence of breach of an intervention order.⁵⁹ Police also use participant monitoring when gathering evidence for criminal prosecutions.⁶⁰
- 6.60 In those Australian jurisdictions where participant monitoring is unlawful (NSW, Western Australia, ACT, South Australia and Tasmania), the legislation contains a range of exceptions. A common exception is where all parties to the conversation or activity consent.⁶¹ Other exceptions are outlined directly below.

When reasonably necessary for the protection of lawful interests

- 6.61 NSW, Tasmania, ACT, Western Australia and South Australia allow participant monitoring by a principal party to the conversation or activity if it is reasonably necessary for the protection of that party's lawful interests.⁶² A principal party is one who speaks or is spoken to in the course of the conversation, or who takes part in the activity.⁶³
- 6.62 The NSW Court of Criminal Appeal has interpreted 'reasonably necessary for the protection of the lawful interests' of a principal party narrowly in order to prevent the exception from swallowing the rule.⁶⁴

50 Ibid.

51 *Guardianship and Administration Act 1986* (Vic) s 37.

52 Section 6 of the SDA prohibits a person using a listening device to monitor a private conversation to which the person is not a party. Section 7 contains a similar prohibition on the use of an optical surveillance device.

53 *Surveillance Devices Act 2001* (Vic) s 11(1).

54 Note that a person's conversation might also be secretly recorded by an individual acting for the police. Specifically, the SDA allows a law enforcement officer, without a warrant, to use a listening device to monitor or record a private conversation to which he or she is not a party if at least one party to the conversation consents, and where the officer is acting in the course of his or her duty and believes the recording is needed to protect the safety of any person: *Surveillance Devices Act 2001* (Vic) s 6(2)(c).

55 This is what was found to have occurred in *Giller v Procopets* (2008) 40 Fam LR 378; [2008] VSCA 236.

56 Victorian Law Reform Commission, *Surveillance in Public Places*, Consultation Paper No 7 (2009) [6.134]; and see *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.

57 *Surveillance Devices Act 1999* (Vic) s 6(1); *Invasion of Privacy Act 1971* (Qld) s 43(1)(a); *Surveillance Devices Act 2007* (NT) s 11(1a).

58 Australian Law Reform Commission, *Privacy*, Report No 22 (1983) [1129].

59 Submission 4.

60 Submission 11.


61 *Surveillance Devices Act 2007* (NSW) s 7(3)(a); *Surveillance Devices Act 1998* (WA) ss 5(3)(c), 6(3)(a); *Listening Devices Act 1992* (ACT) s 4(3)(a); *Listening Devices Act 1991* (Tas) s 5(3)(a).

62 *Surveillance Devices Act 2007* (NSW) s 7(3)(b)(i); *Listening Devices Act 1991* (Tas) s 5(3)(b)(i); *Listening Devices Act 1992* (ACT) s 4(3)(b)(i); *Surveillance Devices Act 1998* (WA) ss 5(3)(c), 6(3)(iii); *Listening and Surveillance Devices Act 1972* (SA) s 7(1)(b).

63 See eg, *Surveillance Devices Act 1998* (WA) s 3 ('principal party').

64 *Sepulveda v R* (2006) 167 A Crim R 108; [2006] NSWCCA 379.

Modernising the Surveillance Devices Act

- 
- 6.63 Although 'reasonably necessary' means only 'reasonably appropriate' (rather than essential),⁶⁵ the Court held that it was not reasonably appropriate for a sexual assault victim to secretly record the perpetrator admitting to the assault. This was because the victim could have approached the police with his complaints.⁶⁶
- 6.64 Thus, the exception does not allow for 'covert recordings of a conversation by any person who alleges that he or she is a victim of crime, and who speaks to the alleged offender for the purpose of obtaining admissions of offences'.⁶⁷
- 6.65 Moreover, what is reasonably necessary is an objective test, having regard to the circumstances that existed at the time the recording was made.⁶⁸ Thus, it is not sufficient that the surveillance user believed it to be reasonably necessary to protect a lawful interest. The Court also declined to give the term 'lawful interests' a broad meaning.⁶⁹ It held that 'lawful interests' do not include an interest in vindicating one's right not to be a victim of crime.⁷⁰

Police duties

- 6.66 NSW, Tasmanian, Western Australian and South Australian⁷¹ surveillance device legislation also exempts participant monitoring by law enforcement officers from the general prohibition against participant monitoring. In the Western Australian legislation, the prohibition against recording a private conversation or a private activity to which a person is a party does not apply to a police officer acting in the course of his or her duty.⁷² Moreover, the Act also exempts a person who acts under instruction from a law enforcement officer in the course of investigating a criminal offence.⁷³ There is a similar provision in the South Australian legislation.⁷⁴
- 6.67 NSW and Tasmania⁷⁵ have broader exemptions. For example, the NSW legislation exempts a law enforcement officer who is a party to a private conversation and is participating in an authorised operation (within the meaning of the *Law Enforcement (Controlled Operations) Act 1997* (NSW)) under an assumed name from the prohibition on the installation, use and maintenance of a listening device.⁷⁶

Other allowed instances of participant monitoring

- 6.68 A number of states (NSW, ACT and Tasmania) also allow for participant monitoring by a principal party when the purpose of the recording is not to share it with individuals who are not a party to the conversation or activity.⁷⁷
- 6.69 The Tasmanian legislation contains a general exception to the ban on the use of a listening device without consent, where the use is to gain evidence or information in connection with an imminent threat of serious violence, substantial damage to property or serious narcotics offence.⁷⁸ In such a case, the user must report to the Chief Magistrate within three days after using the device.⁷⁹ The South Australian legislation allows for participant monitoring if it is 'in the public interest'.⁸⁰

Submissions

- 6.70 There was support in submissions for the proposal in our Consultation Paper that Victoria should prohibit participant monitoring using surveillance devices.⁸¹ Liberty Victoria, for example, noted that the reform would promote privacy and consistency between jurisdictions, bringing provisions of the SDA in line with NSW, South Australia, Tasmania, Western Australia and ACT.⁸²

- 6.71 Those who opposed any change noted the beneficial uses of participant monitoring. For example, Victoria Police argued that the use of participant monitoring enables police to perform important functions such as evidence gathering and the protection of undercover operatives.⁸³ The Lilydale Centre Safe Committee noted its use by parties in domestic violence and family law matters, such as a woman recording her ex-husband's conversations with her as evidence of him breaching his intervention order.⁸⁴ In fact, the Committee favours such monitoring by both parties, because when they do they 'tend to be civil to one another averting further breaches and allegations of breaches'.⁸⁵
- 6.72 One submission suggested that the ban on participant monitoring was ultimately uncontroversial given the prohibition on communicating or publishing the information gained. In consultation with media representatives the commission was told that extending the participant monitoring ban would have little effect on journalistic practices. As one television news executive told the commission, whether participant monitoring should be banned is an academic point because, as it stands, the material obtained through participant monitoring cannot be used.⁸⁶
- 6.73 In general, submissions in favour of the ban also supported exemptions that would allow participant monitoring in limited circumstances. For example, the St Kilda Legal Service said there should be an exception to allow for evidence gathering in family violence and family law matters:
- Without [such an exemption] individuals may find it more difficult to gather evidence to support their case. This is because in family violence matters, for example, there are often no witnesses to the alleged abuse apart from the victim and the perpetrator.*⁸⁷
- 6.74 Liberty Victoria supported the exceptions now found in the SDA (NSW) 'which ensure the practice remains legal in limited and appropriate circumstances'.⁸⁸ The Office of the Victorian Privacy Commissioner went further, suggesting it would be preferable if the exceptions were warrant-based.⁸⁹
- 6.75 The commission is of the view that, as a rule, a person should be able to conduct private conversations and engage in private activities without those events being recorded without their consent. Such an expectation is consistent with the overall purpose of surveillance devices legislation, which is to protect privacy by prohibiting the covert use of surveillance devices other than in exceptional circumstances associated with law enforcement. We recommend that the general participant monitoring exception in sections 6(1) and 7(1) of the SDA be removed.
- 6.76 We accept, however, that in some circumstances this general rule should not apply. Any exceptions to a general prohibition against participant monitoring should not greatly diminish the usual expectation that conversations and activities should not be covertly recorded by anyone.
- 6.77 There is no need to prohibit participant monitoring when all parties to the conversation or activity consent. The prohibitions in the SDA already provide an exception when each party to a conversation or activity gives their consent, express or implied, to the use of a surveillance device.⁹⁰ Consequently, even if the words 'to which the person is not a party' are removed from sections 6(1) and 7(1), there is no need to create an additional exception for those instances when each party has given his or her consent to the recording.

- 65 Meaning that surveillance was the only means by which a person could protect the lawful interest: *Sepulveda v R* [2006] NSWCCA 379 [117].
- 66 *Sepulveda v R* [2006] NSWCCA 379 [139].
- 67 *Sepulveda v R* [2006] NSWCCA 379 [142]. But see *R v Riganias* (2009) 9 DCLR (NSW) 235; [2009] NSWDC 216 where the court found it reasonably necessary for the protection of lawful interests the secret recording by an investor of conversations with an individual to whom he gave money and who he believed may not have been properly investing his money.
- 68 *Sepulveda v R* [2006] NSWCCA 379 [139]. See also *R v Riganias* [2009] NSWDC 216 [13].
- 69 *Sepulveda v R* [2006] NSWCCA 379 [141].
- 70 *Sepulveda v R* [2006] NSWCCA 379 [135], [142].
- 71 *Listening and Surveillance Devices Act 1972* (SA) s 7(1)(b).
- 72 *Surveillance Devices Act 1998* (WA) ss 5(3)(a), 6(3)(b)(i).
- 73 *Surveillance Devices Act 1998* (WA) ss 5(3)(b), 6(3)(b)(ii).
- 74 *Listening and Surveillance Devices Act 1972* (SA) s 7(2).
- 75 *Listening Devices Act 1991* (Tas) s 5(2)(e).
- 76 *Surveillance Devices Act 2007* (NSW) s 7(4)(1).
- 77 *Surveillance Devices Act 2007* (NSW) s 7(3)(b)(ii); *Listening Devices Act 1991* (Tas) s 5(3)(b)(ii); *Listening Devices Act 1992* (ACT) s 4(3)(b)(ii).
- 78 *Listening Devices Act 1991* (Tas) s 5(2)(c).
- 79 *Listening Devices Act 1991* (Tas) s 5(4)-(7).
- 80 *Listening and Surveillance Devices Act 1972* (SA) ss 4, 7(1).
- 81 Submissions 2, 5, 14, 29, 33.
- 82 Submission 5.
- 83 Submission 11.
- 84 Submission 4.
- 85 Submission 4.
- 86 Consultation 12.
- 87 Submission 14.
- 88 Submission 5.
- 89 Submission 29.
- 90 *Surveillance Devices Act 1999* (Vic) ss 6(1), 7(1).

Modernising the Surveillance Devices Act

- 6.78 Participant monitoring by a principal party to a conversation should be possible where it is reasonably necessary for the protection of that party's lawful interests. This exception should not be too broad. For example, we do not favour the exception recently suggested by the New Zealand Law Commission, which would permit non-consensual recording of a conversation to keep a more accurate record than memory could provide.⁹¹
- 6.79 Although we favour a narrow view of the 'lawful interests' exception, we suggest that it should not be as narrow as the one suggested by the NSW Court of Criminal Appeal. We favour an interpretation that allows for participant monitoring for evidentiary purposes, as suggested in a number of the submissions we discussed above.
- 6.80 Similarly, although we support allowing participant monitoring by law enforcement officers in the course of their duties and without a warrant, we favour limiting the exception to situations in which an officer reasonably suspects the person being recorded has committed an offence or is doing so.
- 6.81 We have not proposed the exception found in legislation elsewhere that permits a person to engage in covert participant monitoring when the recording is made without the purpose of sharing the material with others. In these circumstances it is still possible that recordings made by a party to a conversation or activity may fall into the hands of third parties. We have also chosen not to recommend a broad public interest exception because its scope is too uncertain for use in a regime that contains criminal sanctions.

RECOMMENDATION

18. Sections 6 and 7 of the SDA should be amended to prohibit participant monitoring using a listening or optical surveillance device subject to the following additional exceptions:
- a. the use of a listening or optical surveillance device by a law enforcement officer to record a private conversation or private activity to which he or she is a party if:
 - i) the law enforcement officer is acting in the course of his or her duty; and
 - ii) the law enforcement officer reasonably believes at least one party to the conversation or activity of having committed or being in the course of committing an offence
 - b. the use of a listening device or optical surveillance device by a party to a private conversation or private activity if:
 - i) a principal party to the conversation or activity consents to the listening device being so used; and
 - ii) recording of the conversation or activity is reasonably necessary for the protection of the lawful interests of that principal party.

A CIVIL PENALTY REGIME

- 6.82 The SDA provides criminal sanctions when a person uses a surveillance device, or publishes information gained by the use of a surveillance device, in prohibited ways.⁹² The more serious offences attract a maximum penalty of two years imprisonment, or a fine of up to 240 penalty units for an individual (1200 penalty units for a corporation), or both.⁹³
- 6.83 The commission has only been able to find evidence of four successful prosecutions for breach of the SDA since its inception on 1 January 2000. All cases concerned the unlawful use of optical surveillance devices in particularly offensive circumstances.⁹⁴ One explanation for the small number prosecutions may be that the criminal sanctions in the SDA are too severe for use in cases where the wrongful behaviour is not highly offensive.
- 6.84 There is growing support for the use of civil penalties when dealing with many violations of the law. One legislator noted ‘a modern complex society with limited judicial resources and an economic need for efficiency must necessarily seek mechanisms for the enforcement of its rules additional to traditional criminal processes’.⁹⁵ In 2007 the Commonwealth Attorney-General’s Department stated 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.⁹⁶
- 6.85 These matters were considered by the ALRC when it recommended a civil penalties regime for breaches of the *Privacy Act 1988* (Cth).⁹⁷ 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’.⁹⁸
- 6.86 In our Consultation Paper we suggested the introduction of a civil penalty regime for existing offences in the SDA. This would allow a surveillance regulator to act on the less serious matters that come to his or her attention without referring the matter to Victoria Police.
- 6.87 Introducing civil penalties is also likely to reduce the cost and complexity of the regulatory process.⁹⁹ 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’.¹⁰⁰
- 6.88 A number of federal oversight bodies have the power to bring civil penalty proceedings, including the Australian Competition and Consumer Commission (ACCC),¹⁰¹ Australian Securities and Investment Commission (ASIC)¹⁰² and the Environment Protection Authority (EPA).¹⁰³ Civil penalty orders are available under many pieces of Commonwealth legislation.¹⁰⁴
- 6.89 In Victoria, there has also been growing use of civil penalties. For example, the Essential Services Commission is responsible for bringing civil penalty proceedings under a number of Acts, including the *Essential Services Commission Act 2001* (Vic),¹⁰⁵ the *Rail Corporations Act 1996* (Vic),¹⁰⁶ and the *Victorian Renewable Energy Act 2006* (Vic).¹⁰⁷ The courts may make a civil penalty order under the *Outworkers (Improved Protection) Act 2003* (Vic)¹⁰⁸ and the *Long Service Leave Act 1992* (Vic).¹⁰⁹ VCAT may make a civil penalty order under the *Owners Corporation Act 2006* (Vic).¹¹⁰

- 91 New Zealand Law Commission, above n 33 [3.87].
- 92 *Surveillance Devices Act 1999* (Vic) ss 6–12.
- 93 *Surveillance Devices Act 1999* (Vic) ss 6(1), 7(1), 8(1). The penalty unit rate is \$116.82 for the financial year 2009–10. Thus, the current maximum fine for an individual is \$26836.80 and the maximum fine for a body corporate is \$140184.
- 94 See Mark Russell, ‘Privacy Threatened by Hidden Cameras’, *The Age* (Melbourne), 30 September 2009, 2; ‘Former Drama Teacher Pleads Guilty to Porn Charges’, *The Age* (Melbourne), 1 March 2010, 8; Steve Butcher, ‘Man May Face Jail For Pointing Camera at Woman in Toilet’, *The Age* (Melbourne), 4 March 2010, 10.
- 95 Eamonn Moran, ‘Enforcement Mechanisms (including Alternatives to Criminal Penalties)’ (2009) 2 *The Loophole* 12.
- 96 Australian Government, Attorney-General’s Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (December 2007) 63–4.
- 97 The ALRC recommended the *Privacy Act 1988* (Cth) 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, above n 16 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).
- 98 *Ibid* [50.50].
- 99 Australian Law Reform Commission, *Principled Regulation: Federal Civil and Administrative Penalties in Australia*, Report No 95 (2002) [2.81].
- 100 Department of Treasury and Finance, *Victorian Guide to Regulation* (2nd ed, 2007) i.
- 101 Under the *Trade Practices Act 1974* (Cth).
- 102 Under the *Corporations Act 2001* (Cth).
- 103 Under the *Environmental Protection and Biodiversity Conservation Act 1999* (Cth).
- 104 Including the *Banking Act 1959* (Cth) and the *Fair Work (Registered Organisations Act) 2009* (Cth).
- 105 *Essential Services Commission Act 2001* (Vic) s 54A.
- 106 *Rail Corporations Act 1996* (Vic) ss 68–9.
- 107 *Victorian Renewable Energy Act 2006* (Vic) s 71.
- 108 *Outworkers (Improved Protection) Act 2003* (Vic) s 47.
- 109 *Long Service Leave Act 1992* (Vic) s 88.
- 110 *Owners Corporation Act 2006* (Vic) s 166.

Modernising the Surveillance Devices Act

- 6.90 There was broad support for the introduction of a civil penalty regime among submissions to the commission. The Victorian Privacy Commissioner argued that one reason the current criminal regime was ineffective was due to an inherent conflict of interest: the police who prosecute illegal uses of surveillance devices also have an interest in obtaining footage from third parties to assist their investigations.¹¹¹
- 6.91 The Federation of Community Legal Centres supported civil penalties but also promoted an educational approach.¹¹² Victoria Police noted they seek 'protection from liability for police officers acting for a lawful purpose in the course of their duties'.¹¹³
- 6.92 The commission believes that a greater range of regulatory measures should be available to control the use of surveillance in Victoria.
- 6.93 In our Consultation Paper we noted it may be appropriate to retain criminal penalties in the SDA if a civil penalties regime is introduced. The introduction of civil penalties should not restrict police from pursuing criminal prosecutions under the existing provisions of the SDA, or for surveillance-related offences in other Acts. This includes those dealing with stalking,¹¹⁴ indecent, offensive or insulting behaviour¹¹⁵ and 'upskirting'.¹¹⁶ A number of federal regulators, including the ACCC¹¹⁷, ASIC¹¹⁸ and the EPA, have the power to bring civil penalty proceedings when criminal prosecutions are also available.¹¹⁹

RECOMMENDATION

19. Sections 6–9 and 11–12 of the SDA should be amended to include civil penalties as an alternative to criminal penalties. The regulator should be permitted to commence proceedings for the imposition of a civil penalty.

A NEW OFFENCE FOR IMPROPER USE OF A SURVEILLANCE DEVICE

- 6.94 The SDA currently regulates the use of four types of devices: listening devices, optical surveillance devices, tracking devices and data surveillance devices.¹²⁰ The commission has recommended changes to modernise these provisions and to fill gaps that have become apparent over time. In addition, we have considered whether the SDA should be amended to include a new offence that would prohibit offensive surveillance practices regardless of the type of device actually used. The primary purpose of such a new offence would be to send a clear message to the community that various forms of behaviour with a surveillance device are unacceptable.
- 6.95 A number of submissions noted the desirability of ensuring the SDA is sufficiently flexible to cover new and emerging uses of surveillance.¹²¹ Although the commission agrees with these views, it is difficult to prohibit particular uses of unknown devices with the precision necessary for a criminal offence. The commission has concluded, however, that there is merit in introducing a new offence which prohibits unacceptable behaviour with a surveillance device.

- 6.96 The commission is aware of a number of instances of surveillance devices being used to intimidate, demean or harass people. For example, in submissions and consultations we learnt about individuals filming violence for entertainment—a practice known colloquially as ‘happy slapping’. For example, in 2007 a group of young people lured a teenage girl to a park and sexually assaulted her, set fire to her hair and urinated on her.¹²² They filmed the incident and distributed the footage on DVD.¹²³ Other examples include an incident at a secondary school in Pakenham, where a fight between students was recorded on another student’s mobile phone.¹²⁴ Other school yard assaults have also been captured on mobile phone cameras, with those behind the camera audibly encouraging the violence.¹²⁵ In some cases the use of a surveillance device may exacerbate criminal behaviour. For example, in one case, it was reported that a man waved at a camera during a sexual assault.¹²⁶
- 6.97 The fact that the images can be distributed widely and quickly further compounds the problem. One academic stated that ‘the internet actually encourages this behaviour because kids from all over the world go on and rate the fights, so ... this particular medium may be encouraging violence’.¹²⁷
- 6.98 Surveillance devices can be used to record highly personal information. In a recent case, *Giller v Procopets*,¹²⁸ the defendant covertly filmed the couple’s consensual sexual activity and later threatened to show the plaintiff’s family and friends the videotapes. This sort of behaviour should be strongly discouraged.
- 6.99 In Chapter 4 we also noted media reports of an increase in individuals using devices such as camera phones to capture images of other people in distress during emergencies. Recent examples include incidents in which people have filmed the aftermath of traffic accidents.¹²⁹ In one instance, onlookers filmed the dying moments of a man after a car hit him.¹³⁰ Filming an emergency in order to assist emergency services is quite different to filming an emergency for entertainment purposes.

- 111 Submission 29.
 112 Submission 40.
 113 Submission 11.
 114 *Crimes Act 1958* (Vic) s 21A.
 115 *Summary Offences Act 1966* (Vic) s 17.
 116 *Summary Offences Act 1966* (Vic) ss 41A, 41B, 41C.
 117 Under the *Trade Practices Act 1974* (Cth).
 118 Under the *Corporations Act 2001* (Cth).
 119 Under the *Environmental Protection and Biodiversity Conservation Act 1999* (Cth).
 120 *Surveillance Devices Act 1999* (Vic) ss 6–9.
 121 Submissions 11, 29, 33, 36.
 122 Mex Cooper, ‘Werribee DVD Sex Case: Teens’ Attack Sickening, Says Girls Dad’, *Geelong Advertiser* (Geelong), 18 October 2007 <www.geelongadvertiser.com.au/article/2007/10/18/7951_news.html> at 18 November 2009; Greg Roberts, ‘Boys Escape Detention Over Assault Film’, *The Age* (Melbourne), 5 November 2007 <<http://news.theage.com.au/national/boys-escape-detention-over-assault-film-20071105-18ct.html>> at 18 November 2009.
 123 See Cooper, above n 122.
 124 Anthony Dowsley, ‘Schoolboy Filmed by Classmates Being Bashed’, *Herald Sun* (Melbourne), 15 October 2009, 4.
 125 See eg, Alyssa Betts, ‘Boxing Champ Filmed in School Bashing’, *NT News* (Darwin), 4 December 2009 <www.ntnews.com.au/article/2009/12/04/106431_ntnews.html> at 22 January 2010.
 126 ‘Pair Jailed for Drugging, Raping 14-Year-Old Girls’, *The Age* (Melbourne), 8 December 2009 <www.theage.com.au/national/pair-jailed-for-drugging-raping-14yearold-girls-20091208-kgb0.html> at 21 January 2010. See also ‘Gang Sex Attack Filmed on Mobile Phone’, *The Age* (Melbourne), 17 May 2007 <<http://news.theage.com.au/national/gang-sex-attack-filmed-on-mobile-phone-20070517-db9.html>> at 18 November 2009.
 127 Professor Kerry Carrington quoted in Robyn Ironside, ‘Girl Fight Videos Posted on Internet Amid Violence Surge’, *The Courier-Mail* (Brisbane), 12 January 2010 <www.news.com.au/national/girl-fight-videos-posted-on-internet-amid-violence-surge/story-e6frfkvr-1225818238872> at 22 January 2010.
 128 (2008) 40 Fam LR 378; [2008] VSCA 236. The court awarded Ms Giller a total of \$135,000 in damages.
 129 Gemma Jones and Anna Caldwell, ‘Onlookers Film Burning Car as Sisters Lay Dying’, *Courier Mail* (Brisbane), 30 December 2009 <www.news.com.au/couriermail/story/0,23739,26535799-952,00.html> at 25 January 2010; Peter Michael, ‘Police Condemn Ghoulis People Who Filmed Backpacker’s Dying Moments’, *Courier Mail* (Brisbane), 8 January 2010 <www.news.com.au/national/police-condemn-ghoulis-people-who-filmed-backpackers-dying-moments/story-e6frfkvr-1225817200736> at 25 January 2010.
 130 Michael, above n 129.

Modernising the Surveillance Devices Act

- 6.100 Sometimes surveillance devices are used for the purpose of intimidation or to prevent people from doing something they are otherwise lawfully entitled to do. Some submissions to our Consultation Paper expressed concern about surveillance being used in this manner.¹³¹ Local examples include anti-abortion campaigners setting up surveillance outside abortion clinics and people being filmed entering gay bars or drug treatment clinics.¹³²
- 6.101 In consultations and submissions concern was expressed at the power relationship that exists between users of surveillance and people under surveillance.¹³³ At the extreme end of the scale, classic cases of blackmail involve the threat of the release of personal or embarrassing information. Submissions gave examples of people involved in an embarrassing incident who have been recorded, and then the footage later broadcast on television or uploaded to the internet.¹³⁴

OTHER JURISDICTIONS

- 6.102 Some other countries have criminalised the act of filming violence for entertainment. For example, in 2007, the French government inserted provisions into its criminal code as a response to the rising incidences of ‘happy slapping’.¹³⁵ Now, only professional journalists may film real-world violence and distribute it on the internet.¹³⁶ The offence is punishable by up to five years imprisonment and/or a fine of up to €75 000.¹³⁷
- 6.103 The New Zealand Law Commission has recently delivered its final report into invasion of privacy. Recommendations include strengthening and streamlining prohibitions against inappropriate uses of surveillance devices. For example, the Commission recommends that the sections of the *Crimes Act 1961* (NZ) dealing with intimate visual recordings (which aim to prevent the filming of a person’s sexual activity or intimate areas without their consent)¹³⁸ should be moved into their proposed new Surveillance Devices Act.¹³⁹ Further, the Commission recommends that ‘keeping a person under surveillance’ should be added as a specified form of surveillance regulated under the *Harassment Act 1997* (NZ).¹⁴⁰
- 6.104 Newspaper articles from the UK cite particularly violent incidents of happy slapping,¹⁴¹ including instances in which a victim ultimately died from their injuries.¹⁴² In the UK there is no specific offence prohibiting filming violent attacks for entertainment, however, other offences may be used to deal with this behaviour. In 2008 a teenager who used her mobile phone to film the fatal bashing of a man pleaded guilty to aiding and abetting manslaughter, even though she did not physically participate in the attack. She was sentenced to two years imprisonment.¹⁴³
- 6.105 The commission is of the view that it is desirable to introduce a new offence that demonstrates clear community disapproval of the growing use of a surveillance device to intimidate, demean or harass people. There is considerable educative value in a strong legislative statement that it is unacceptable to use a surveillance device for these purposes. Although there are already some offences concerning certain specific uses of surveillance devices, such as stalking or ‘upskirting’, and while offensive behaviour of any nature in a public place is unlawful,¹⁴⁴ there is no specific offence concerned with the grossly offensive use of a surveillance device.

- 6.106 The SDA currently prohibits the publication or recording of a private conversation or private activity.¹⁴⁵ The current SDA prohibitions are limited to private conduct. These provisions do not apply where parties ought reasonably to expect that someone else could observe what they are doing or saying.¹⁴⁶ Many of the inappropriate uses of surveillance devices would probably constitute an offence of obscene, indecent or offensive behaviour under the *Summary Offences Act 1966* (Vic).¹⁴⁷ This longstanding offence does not provide the community with a clear message, however, that use of a surveillance device to intimidate, demean or harass another person is unacceptable. The commission is of the view that a separate offence in the SDA would appropriately serve this purpose.
- 6.107 The new offence should apply in two situations. First, where a surveillance device is used to intimidate, demean or harass a person of ordinary sensibilities. Secondly, where a surveillance device is used to prevent or hinder a person from performing an act they are lawfully entitled to do. This latter situation includes, for example, using a surveillance device to discourage people from entering places such as abortion clinics or gay bars.
- 6.108 Some submissions expressed concern that any amendments to the SDA should avoid criminalising legitimate uses of surveillance devices.¹⁴⁸ We believe that the proposed new offence strikes an appropriate balance and would not outlaw acceptable uses of surveillance devices. For example, the use of a surveillance device by the media to record the aftermath of a natural disaster is part of their legitimate newsgathering activity, and is not conducted for the purpose of intimidating, demeaning or harassing an individual.

RECOMMENDATION

20. A new offence should be included in the SDA that makes it unlawful to use a surveillance device in such a way as to:
- intimidate, demean or harass a person of ordinary sensibilities; or to
 - prevent or hinder a person of ordinary sensibilities from performing an act they are lawfully entitled to do.
21. A civil and alternative criminal penalty should apply for breach of the offence. The regulator should be permitted to commence proceedings for the imposition of a civil penalty.

CONCLUSION

- 6.109 At present the SDA regulates the use of surveillance devices inconsistently—certain activities are prohibited while others are effectively permitted because the Act says nothing about them. Furthermore, breaches of the Act attract serious criminal sanctions, which have proven not particularly effective in regulating public place surveillance. In this chapter we have explained our recommended changes to the Act to address these shortcomings, and to modernise the way in which the use of surveillance devices is regulated.

- 131 Submissions 5, 33.
 132 Submission 6; Forum 1.
 133 Submission 14.
 134 Submission 5.
 135 'France: New Law Says Only Scribes can Upload Violence Snaps', *The Times* (India), 8 March 2007 <www.asiamedia.ucla.edu/article.asp?parentid=65364> at 22 January 2010.
 136 *Legifrance, Law No 2007-297 of 5 March 2007* (2010) <www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000615568&dateTexte=> at 3 February 2010.
 137 *New Prevention of Criminality Law Poses Threat to Citizen Reporting* (2007), Reporters Without Borders <www.rsf.org/New-prevention-of-criminality-law.html> at 27 January 2010.
 138 *Crimes Act 1961* (NZ) ss 216G–216N.
 139 New Zealand Law Commission, above n 33, rec 6.
 140 *Ibid* rec 21.
 141 See eg, a recent case in which two brothers tortured four people over several hours, one of whom nearly died. 'Edlington: Full Text of Mr Justice Keith's Comments to Torture Brothers', *The Times Online* (London), <www.timesonline.co.uk/tol/news/uk/crime/article6998667.ece> at 25 January 2010.
 142 "'Happy Slapper' Killers Jailed' (8 July 2007) *ABC News* <<http://abc.gov.au/news/stories/2007/07/28/1990731.htm>> at 25 January 2010.
 143 Angela Balakrishnan, *Girl Jailed for Filming "Happy Slap" Killing* (18 March 2008) *guardian.co.uk* <www.guardian.co.uk/uk/2008/mar/18/happyslap.killing> at 25 January 2010.
 144 *Summary Offences Act 1966* (Vic) div 4A; *Crimes Act 1958* (Vic) s 21A.
 145 *Surveillance Devices Act 1999* (Vic) s 11.
 146 *Surveillance Devices Act 1999* (Vic) ss 3, 11.
 147 *Summary Offences Act 1966* (Vic) s 17.
 148 Submissions 7, 19.

Chapter 7

Statutory Causes of Action

WARNING
**PREMISES UNDER
CONSTANT
SURVEILLANCE**

CONTENTS

- 128 Introduction
- 128 Civil action for serious invasions of privacy
- 141 Other law reform commission recommendations
- 145 Should Australia enact a cause of action for invasion of privacy?
- 147 The commission's recommendation: two statutory causes of action
- 167 Conclusion

INTRODUCTION

- 7.1 One of the options discussed in our Consultation Paper is a statutory cause of action¹ for a serious invasion of privacy. In the interests of national consistency, we suggested that the cause of action for a serious invasion of privacy recommended by the Australian Law Reform Commission (ALRC) in 2008 could be used as the model for any new Victorian law.²
- 7.2 The ALRC recommended that its proposed cause of action be included in Commonwealth legislation.³ Any such legislation would probably remove Victoria's ability to enact a similar cause of action because of constitutional restrictions.⁴ However, as the Commonwealth may not implement the ALRC's recommendation, or may take some time to do so,⁵ Victoria is still in a position to provide leadership in this area.
- 7.3 Since the release of the ALRC report, the NSW Law Reform Commission (NSWLRC) has recommended a different version of a statutory cause of action for invasion of privacy.⁶ Consequently, national harmony in this field may be a long-term goal.
- 7.4 This chapter begins with a summary of the relevant law in Australia and other comparable jurisdictions. We then discuss the views of those who made submissions about our Consultation Paper proposal. The Consultation Paper proposal attracted support and opposition. Some supporters also suggested different causes of action to that proposed by the ALRC.
- 7.5 We recommend the introduction of two statutory causes of action for serious invasions of privacy: the first dealing with misuse of private information, the second with intrusion upon seclusion. Although our focus is an appropriate legal response to the misuse of surveillance in public places, these new causes of action would not necessarily be limited to conduct that occurred in a public place or that involved the use of a surveillance device. We have drawn upon the work of the ALRC and the NSWLRC when devising these causes of action.
- 7.6 Our recommendations deal with the legal characterisation of these causes of action, their elements, the defences, the remedies, the people granted rights by the law, the limitations period, and the tribunal that should hear these cases.

CIVIL ACTION FOR SERIOUS INVASIONS OF PRIVACY

THE LAW IN AUSTRALIA

- 7.7 The right of a person to take civil action for a serious invasion of privacy by use of a surveillance device in a public place is unclear. There are no relevant statutory causes of action for invasion of privacy in any Australian jurisdiction.⁷ No appellate court has acknowledged the existence of a common law tort of invasion of privacy.⁸ The availability of general law causes of action, such as a claim for breach of confidence, which has been used in other countries⁹ to seek redress for a serious invasion of privacy in a public place, is untested.¹⁰
- 7.8 The common law regulates some surveillance activities, but does so indirectly when protecting other interests, most particularly those in property. The interest most directly and immediately affected by surveillance activities—privacy—has not received much attention from the common law. 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.*¹¹

7.9 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 different practices involved’ and because the proper balance to be struck between the diverse interests ‘varies greatly and demands individualised solutions’.¹² Former Chief Justice of the Australian High Court Murray Gleeson has referred to ‘the lack of precision of the concept of privacy’ and to ‘the tension that exists between interests in privacy and interests in free speech’.¹³ The limited capacity of the traditional common law remedies to deal with the damage caused by invasion of privacy may have also contributed to the fact that there have been few privacy cases to assist in the formulation of broad principles.¹⁴

7.10 Although no decision of the High Court, or of any Australian intermediate appellate court, has confirmed the existence of an Australian tort of invasion of privacy, in 2001 various members of the High Court observed that there is no barrier to the creation of such a tort.¹⁵ As two members of the New Zealand Court of Appeal subsequently pointed out, ‘the High Court of Australia has not ruled out the possibility of a common law tort of privacy, nor has it embraced it with open arms’.¹⁶

7.11 Since 2001, two Australian trial courts have recognised a tort of invasion of privacy.¹⁷ In *Grosse v Purvis*¹⁸ a judge in the Queensland District Court concluded that a prolonged course of stalking and harassment was an unlawful invasion of the plaintiff’s privacy. The Court decided that the conduct in question was unlawful because it amounted to a breach of ‘the actionable right of an individual person to privacy’.¹⁹

1 A cause of action is a right to sue another person.

2 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 3: Final Report* 108 (2008) rec 74–1.

3 Ibid.

4 S 109 of the Constitution renders a state law inoperative when it is inconsistent with a Commonwealth law. A state law may be inconsistent with a Commonwealth law when the Commonwealth law seeks to be the sole law covering a particular activity. In these circumstances, the Commonwealth law covers the field.

5 On 14 October 2009 Cabinet Secretary Senator Joe Ludwig released the Commonwealth Government’s response to the ALRC’s Report 108. The Commonwealth Government has neither accepted nor rejected the ALRC’s recommendations concerning a statutory cause of action for serious invasions of privacy. It announced that the relevant recommendations will be considered later (Australian Government, *Enhancing National Privacy Protection: First Stage Response to the Australian Law Reform Commission Report 108 ‘For Your Information: Australian Privacy Law and Practice’*, October 2009).

6 NSW Law Reform Commission, *Invasion of Privacy*, Consultation Paper No 1 (2007), 3.

7 See Chapter 3 for a brief discussion of compensation awards for information privacy breaches.

8 See *Australian Broadcasting Corporation v Lenah Game Meats Pty Limited* (2001) 208 CLR 199 [132].

9 See eg, the House of Lords decision in *Campbell v MGN Ltd* [2004] 2 AC 457.

10 Recent appellate court decisions concerning the reach of the action for breach of confidence involved the use of a surveillance device (a video camera) in private places (see *Australian Broadcasting Corporation v Lenah Game Meats Pty Limited* (2001) 208 CLR 199 [34]–[39]; *Giller v Procopets* [2008] 40 Fam LR 378.

11 Danuta Mendelson, *The New Law of Torts* (2007) 6.

12 John Fleming, *The Law of Torts* (9th ed, 1998) 665.

13 *Australian Broadcasting Corporation v Lenah Game Meats Pty Limited* (2001) 208 CLR 199 [41].

14 See *Giller v Procopets* [2008] 40 Fam LR 378 for discussion of the available remedies.

15 *Australian Broadcasting Corporation v Lenah Game Meats Pty Limited* (2001) 208 CLR 199. See Ian Callinan, ‘Privacy, Confidence, Celebrity and Spectacle’ (2007) 7 *Oxford University Commonwealth Law Journal* 1.

16 *Hosking v Runting* [2005] 1 NZLR 1 [59] (Gault P and Blanchard J). This statement was made following a detailed consideration of the relevant judgments in *Australian Broadcasting Corporation v Lenah Game Meats Pty Limited* (2001) 208 CLR 199.

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

18 [2003] QDC 151.

19 *Grosse v Purvis* [2003] QDC 151 [442].

- 7.12 The court determined that the essential elements of an action for invasion of privacy are
- a willed act by the defendant*
 - which intrudes upon the privacy or seclusion of the plaintiff*
 - in a manner which would be considered highly offensive to a reasonable person of ordinary sensibilities*
 - and which causes the plaintiff detriment in the form of mental, psychological or emotional harm or distress, or because it prevented or hindered her from doing an act which she was lawfully entitled to do.*²⁰
- 7.13 In *Doe v Australian Broadcasting Corporation*²¹ a Victorian County Court judge held that the publication of the name of a rape victim entitled her to damages for breach of confidence, negligence, breach of statutory duty and invasion of privacy. Judge Hampel observed that the 'development of a tort of invasion of privacy is intertwined with the development of the cause of action for breach of confidence' and that both causes of action are concerned with 'a recognition of the value of, and importance of the law recognising and protecting human dignity'.²² Although Judge Hampel did not consider it appropriate to formulate an exhaustive description of the elements of the cause of action for invasion of privacy, she concluded that the wrong done in the case 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'.²³

Possible common law developments

- 7.14 Despite these trial court decisions, development of a broad ranging tort of invasion of privacy is likely to take a very long time because of the way the common law develops. Although the courts may 'reformulate existing legal rules and principles to take account of changing social conditions',²⁴ there is widespread judicial acceptance of the proposition that 'in a democratic society, changes in the law that cannot logically or analogically be related to existing common law rules and principles are the province of the legislature'.²⁵
- 7.15 In the short term, the Australian High Court may follow the lead of the House of Lords²⁶ and the New Zealand Court of Appeal,²⁷ which have both declined to develop a broad tort of invasion of privacy, but have recognised a more limited cause of action for misuse of private information. In order for this step to occur appropriate cases would need to make their way through the legal system to the High Court.

THE LAW IN THE UK

Misuse of private information

- 7.16 In 2004 the House of Lords declared that there is no common law tort of invasion of privacy in the UK.²⁸ However, the equitable action for breach of confidence, which was originally concerned with the wrongful disclosure of information obtained in a confidential relationship,²⁹ is evolving into a wider action concerned with misuse of private information. The elements and reach of this cause of action, described by one Law Lord as a tort,³⁰ are developing slowly on a case-by-case basis.

7.17 In *Campbell v MGN Ltd*³¹—a case concerning disclosure by a newspaper that model Naomi Campbell had attended a Narcotics Anonymous meeting—the House of Lords confirmed that the action for breach of confidence ‘has now firmly shaken off the limiting constraint of the need for an initial confidential relationship’.³² The court held that the obligation to respect the confidentiality of information extends to a person who knows, or ought to know, that information that he or she receives is confidential.³³ The essence of the action for breach of confidence is now misuse of private information. It seeks to protect ‘two different interests: privacy and secret (confidential) information’.³⁴

7.18 Human rights principles were a catalyst for the common law developments in *Campbell*. In 2003,³⁵ the European Court of Human Rights had found that public disclosure of CCTV footage of a man who had attempted suicide in an English street breached his right to privacy.³⁶ Moreover, it had found that English law provided him with ‘no effective remedy in relation to the violation of his right to respect for his private life guaranteed by Article 8 of the Convention’.³⁷ When *Campbell* was decided in 2004, all of the members of the House of Lords considered European human rights issues.³⁸ Lord Nicholls said that ‘the values enshrined in articles 8 and 10 [of the European Convention on Human Rights] are now part of the cause of action for breach of confidence’ and that change has been achieved ‘by absorbing the rights protected by articles 8 and 10 into this cause of action’.³⁹ Article 8 of the European Convention is concerned with privacy while article 10 is concerned with freedom of expression.⁴⁰ Lord Nicholls went on to say:

*The values embodied in articles 8 and 10 are as much applicable in disputes between individuals or between an individual and a non-governmental body such as a newspaper as they are in disputes between individuals and a public authority.*⁴¹

Elements

7.19 The law concerning the elements, defences and remedies that apply to the cause of action for misuse of private information is embryonic. The elements of the cause of action appear to be, first, ‘whether the claimant had a reasonable expectation of privacy in relation to the particular information in question’ and, secondly, ‘whether there is some countervailing public interest such as to justify overriding that prima facie right’.⁴² Both issues are ‘essentially questions of fact’.⁴³ The English courts have provided limited guidance about matters to consider, or steps to take, when resolving these questions of fact.

7.20 The first element—a reasonable expectation of privacy—involves an objective evaluation of the expectation of ‘a reasonable person of ordinary sensibilities ... placed in the same position as the claimant and faced with the same publicity’.⁴⁴ The Court of Appeal has recently listed a number of factors that can be considered when deciding whether the claimant had a reasonable expectation of privacy.⁴⁵ These include the attributes of the claimant, the nature of the activity he or she was engaged in, the place where it occurred, the nature and purpose of any intrusion, the presence or absence of consent, how the information came into the possession of the publisher, and the effect of publication on the claimant.⁴⁶ Although the courts have warned against generalisations about the sort of behaviour that attracts a reasonable expectation of privacy, in those cases where the claimant has been successful, ‘the information in question has been of a strictly personal nature concerning, for example, sexual relationships, mental or physical health, financial affairs, or the claimant’s family or domestic arrangements’.⁴⁷

- 20 *Grosse v Purvis* [2003] QDC 151 [444].
- 21 [2007] VCC 281. Although an appeal was lodged against the decision, the case was settled before the appeal was heard.
- 22 [2007] VCC 281 [148].
- 23 [2007] VCC 281 [163].
- 24 *Breen v Williams* (1996) 186 CLR 71, 115 (Gaudron and McHugh JJ).
- 25 *Ibid.*
- 26 *Wainright v Home Office* [2004] 2 AC 406 [35] (Lord Hoffman).
- 27 *Hosking v Runting* [2005] 1 NZLR 1 [110] (Gault P and Blanchard J).
- 28 *Wainright v Home Office* [2004] 2 AC 406 [35].
- 29 The elements of the traditional action for breach of confidence were explained by Megarry J in *Coco v A N Clark (Engineers) Ltd* [1969] RPC 41.
- 30 *Campbell v MGN Ltd* [2004] 2 AC 457 [13] (Lord Nicholls). There is uncertainty about whether the cause of action is properly described as a tort, as a majority of the House of Lords in *Campbell* did not formally adopt Lord Nicholls’ characterisation (See eg, *Mosley v News Group Newspapers Limited* [2008] EWHC 177 [184] (QB)).
- 31 [2004] 2 AC 457.
- 32 *Campbell v MGN Ltd* [2004] 2 AC 457 [14] (Lord Nicholls).
- 33 *Campbell v MGN Ltd* [2004] 2 AC 457, [14].
- 34 *Campbell v MGN Ltd* [2004] 2 AC 457, [14]–[15].
- 35 *Peck v United Kingdom* [2003] ECHR 44.
- 36 *Peck v United Kingdom* [2003] ECHR 44 [62]–[63].
- 37 [2003] ECHR 44 [113]. Article 13 of the European Convention of Human Rights requires an effective national remedy for any violation of Convention rights.
- 38 Although the House of Lords was divided (3–2) on the question of whether the plaintiff should succeed on the facts of the case, all five Law Lords supported the development of the cause of action for misuse of private information.
- 39 *Campbell v MGN Ltd* [2004] 2 AC 457 [17].
- 40 Article 8 of the European Convention deals with ‘respect for private and family life’ and Article 10 with ‘freedom of expression’.
- 41 *Campbell v MGN Ltd* [2004] 2 AC 457 [17].
- 42 *The Author of a Blog v Times Newspapers Limited* [2009] EWHC 1358 (QB) [7] (Eady J). An act of the defendant that led to the publication of the information in question appears to be subsumed within these two elements.
- 43 *Murray v Big Pictures (UK) Limited* [2008] EWCA Civ 446 [41] (Clarke MR).
- 44 *Campbell v MGN Ltd* [2004] 2 AC 457 [99] (Lord Hope); *Murray v Big Pictures (UK) Limited* [2008] EWCA Civ 446 [35] (Clarke MR).
- 45 *Murray v Big Pictures (UK) Limited* [2008] EWCA Civ 446 [36] (Clarke MR).
- 46 *Murray v Big Pictures (UK) Limited* [2008] EWCA Civ 446 [36] (Clarke MR).
- 47 *The Author of a Blog v Times Newspapers Limited* [2009] EWHC 1358 (QB) [9] (Eady J).

- 7.21 The second element involves striking a balance between an individual's right to privacy and a publisher's right to publish. Resolving 'the tension between privacy and freedom of expression'⁴⁸ is not easy, as the result in *Campbell* demonstrates. The House of Lords divided 3–2 in favour of the plaintiff on this point. Although no appellate court has yet identified a list of factors to be considered when seeking to strike this balance, it appears that an evaluation of the worth or value of the private information disclosed has been significant in some cases.⁴⁹ In addition, the 'difficult question of proportionality may arise' when considering how to assess any interference with one person's right to privacy or another's freedom of expression.⁵⁰ What this may mean is, for example, that an act done to further one person's right to freedom of expression must not have a disproportionate impact upon another's right to privacy.

Defences

- 7.22 The English courts have not yet articulated any defences to a claim for misuse of private information. It does appear, however, that consent is a defence, just as it is to most torts. There may also be a 'defence'⁵¹ that is quite similar to the defence of qualified privilege in defamation law.⁵² In *Campbell* all five Law Lords accepted that it was quite lawful for the newspaper in question to publish the fact that Naomi Campbell was a drug addict because she had made many public statements to the contrary.⁵³ Lord Nicholls said that 'where a public figure chooses to present a false image and make untrue pronouncements about his or her life, the press will normally be entitled to put the record straight'.⁵⁴

Remedies

- 7.23 It is not clear whether the wrong of misuse of private information requires proof of actual damage or whether, like the tort of trespass, it may be committed without proof of any damage. This lack of clarity has created uncertainty about the types of damages that may be awarded.⁵⁵
- 7.24 Damages awards have generally been modest in these cases, perhaps because the courts have been asked to order compensation for injury that is difficult to assess and quantify. The cause of action seeks 'to protect such matters as personal dignity, autonomy and integrity', and 'damages for such an infringement may include distress, hurt feelings and loss of dignity'.⁵⁶ In *Mosley v News Group Newspapers Limited*, which attracted the largest damages award of £60 000, Eady J said 'an infringement of privacy cannot ever be effectively compensated by a monetary award'.⁵⁷ He also noted that 'once privacy has been infringed, the damage is done and the embarrassment is only augmented by pursuing a court action'.⁵⁸ When concluding that £60 000 was the appropriate sum in the case, Eady J stated that Mr Mosley 'is hardly exaggerating when he says that his life was ruined'.⁵⁹
- 7.25 The British courts have also issued injunctions to prevent the initial publication, or continued publication, of material in some misuse of private information cases. Injunctions have prevented publication of the addresses of convicted murderers once they have been released from prison,⁶⁰ the details of the extra-marital sex life of a football player,⁶¹ the private life of a musician,⁶² and the musings of Prince Charles in his diary.⁶³
- 7.26 By contrast, in the recent case of *John Terry v Persons Unknown*,⁶⁴ the court rejected an application for an injunction to prevent the media from publishing information about an affair between the English football captain and a then-unknown woman. Justice Tugendhat concluded that disclosing the existence of the relationship was not of itself highly intrusive,⁶⁵ and that there was room for argument about the social utility of publishing this information.⁶⁶

Costs

7.27 Even though damages awards have generally been quite small in misuse of private information litigation, costs awards have been quite extraordinary in some of the more notorious cases. Naomi Campbell was awarded damages of £3500 and costs of £1.08 million.⁶⁷ Max Mosley was awarded damages of £60 000 and costs of £850 000.⁶⁸ Costs orders have also outstripped damages awards in some of the significant European Court of Human Rights cases. One man was awarded damages of £11 800 and costs of £18 075 for the broadcasting of CCTV footage of his suicide attempt.⁶⁹

Criticism of the cause of action

7.28 Viewed from one perspective, many of the more prominent English misuse of private information cases are little more than legal actions by celebrities to suppress inconvenient truths. For example, English Law Lord, Baroness Hale, described the *Campbell* case as ‘a prima donna celebrity against a celebrity-exploiting newspaper’,⁷⁰ noting that ‘each in their time has profited from the other. Both are assumed to be grown-ups who know the score’.⁷¹ The New Zealand Law Commission referred to ‘the more highly-developed celebrity culture, and the more aggressive nature of the media, in Britain’ when commenting upon the differences between the types of cases that had arisen in the UK and New Zealand.⁷²

7.29 Some British cases have provided an effective forum, however, to determine the limits that should be placed upon the publication of information obtained by use of surveillance devices. Although people must expect to be observed in many public places, recent UK cases have illustrated conduct that may fall beyond the limits of reasonable exposure to the gaze of others, or to the use of information obtained by the use of a surveillance device in a public place. Is it acceptable, for example, to broadcast CCTV footage of a man who has just slashed his wrists in the street,⁷³ or to publish a photo of a small child—whose mother happens to be a famous author—being pushed down the street in a stroller?⁷⁴

7.30 The English courts have been criticised for distorting settled legal principle because they have been content to develop existing legal rules in response to new situations rather than devise entirely new common law rules as their New Zealand counterparts have done. Butler has questioned

*the legitimacy of the theoretical transformation of an equitable doctrine, based on a confidante’s obligations of good conscience and for which an injunction is the major discretionary remedy, into what is studiously referred to by several judges as the ‘action’ for breach of confidence but which is evidently a tort protecting an aspect of human dignity, the major remedy for which is substantive damages.*⁷⁵

7.31 There is some power to this criticism. Private information may be quite different to confidential information. The traditional equitable action for breach of confidence dealt with the wrongful use of information acquired in the course of a confidential relationship. This cause of action sought to preserve the element of trust that forms part of any confidential relationship. Privacy, however, is concerned with control of information that may never be revealed to anyone. Preservation of human dignity lies at the core of privacy protection. As two members of the New Zealand Court of Appeal said in a leading case:

*Privacy and confidence are different concepts. To press every case calling for a remedy for unwarranted exposure of information about private lives of individuals into a cause of action having as its foundation trust and confidence will be to confuse those concepts.*⁷⁶

- 48 *Campbell v MGN Ltd* [2004] 2 AC 457 [28] (Lord Nicholls).
- 49 See eg, *Campbell v MGN Ltd* [2004] 2 AC 457; *Mosley v News Group Newspapers Limited* [2008] EWHC 177 (QB).
- 50 *Campbell v MGN Ltd* [2004] 2 AC 457 [20] (Lord Nicholls).
- 51 Lord Nicholls suggested that this issue may fall within one of the elements of the cause of action because it may affect the ‘reasonableness’ of the claimant’s expectation of privacy (*Campbell v MGN Ltd* [2004] 2 AC 457 [24]).
- 52 See Patrick George, *Defamation Law in Australia* (2006).
- 53 The case was ultimately fought over the issue of whether it was lawful for the newspaper to publish a photo of Naomi Campbell, covertly taken and at a distance, in a public street, leaving a Narcotics Anonymous meeting as well as details of what occurred at those meetings (*Campbell v MGN Ltd* [2004] 2 AC 457 [23]–[25]).
- 54 *Campbell v MGN Ltd* [2004] 2 AC 457 [24] (Lord Nicholls). Lord Nicholls’ statement can be traced back to the Court of Appeal decision in *Woodward v Hutchins* [1977] 1 WLR 760. For a discussion, see Sam Ricketson, ‘Public Interest and Breach of Confidence’ (1979) 12 *Melbourne University Law Review* 176.
- 55 See eg, *Mosley v News Group Newspapers Limited* [2008] EWHC 177 (QB) [214].
- 56 *Mosley v News Group Newspapers Limited* [2008] EWHC 177 (QB) [214]–[216].
- 57 *Mosley v News Group Newspapers Limited* [2008] EWHC 177 (QB) [231].
- 58 *Mosley v News Group Newspapers Limited* [2008] EWHC 177 (QB) [230].
- 59 *Mosley v News Group Newspapers Limited* [2008] EWHC 177 (QB) [236].
- 60 *Venables v News Group Newspapers Ltd* [2001] Fam 430.
- 61 *A v B plc* [2003] QB 195.
- 62 *McKennitt v Ash* [2008] QB 73.
- 63 *Associated Newspapers Ltd v HRH Prince of Wales* [2008] Ch 105.
- 64 [2010] EWHC 119 (QB).
- 65 [2010] EWHC 119 (QB) [68].
- 66 [2010] EWHC 119 (QB). [102]–[105].
- 67 *Campbell v MGN Ltd Limited* [2005] 2 AC 457.
- 68 ‘Mosley Wins £60 000 in Privacy Case’ *Metro*, 24 July 2008 <www.metro.co.uk/news/article.html?in_article_id=233683&in_page_id=34> at 19 November 2009.
- 69 *Peck v United Kingdom* [2003] ECHR 44.
- 70 *Campbell v MGN* [2004] 2 AC 457 [143].
- 71 *Campbell v MGN* [2004] 2 AC 457 [143].
- 72 New Zealand Law Commission, *Invasion of Privacy: Penalties and Remedies Review of the Law of Privacy Stage 3 Issues Paper No 14* (2009) [4.69].
- 73 *Peck v United Kingdom* [2003] ECHR 44.
- 74 *Murray v Big Pictures (UK) Limited* [2008] EWCA Civ 446.
- 75 Des Butler, ‘A Tort of Invasion of Privacy in Australia?’ (2005) 29 *Melbourne University Law Review* 339, 352.
- 76 *Hosking v Runting* [2005] 1 NZLR 1[48] (Gault P and Blanchard J).

- 7.32 The response to this criticism by one Law Lord has been to observe that the action for breach of confidence has split in two. Lord Nicholls said that ‘the law has developed’ so that ‘breach of confidence, or misuse of confidential information, now covers two distinct causes of action, protecting two different interests: privacy and secret (“confidential”) information’.⁷⁷
- 7.33 The continued development of that branch of the breach of confidence cause of action that protects privacy may be troublesome, however, because as Lord Walker has observed, its ‘uncontrolled growth’ may ‘tend to bring incoherence into the law of intellectual property’.⁷⁸

Intrusion upon seclusion

- 7.34 UK common law has not yet developed a cause of action to protect what is referred to as ‘intrusion upon seclusion’ in United States tort law,⁷⁹ even though British courts have referred to a relevant gap in the law on a number of occasions over the past 20 years. The core of this wrong is an unjustifiable intrusion into a person’s private space, such as the use of a camera to engage in ‘upskirting’ or a hidden device to record a private conversation.
- 7.35 In 1991 the English Court of Appeal found that there was no remedy for invasion of any privacy interest when a journalist and a photographer entered the hospital room of a celebrity without permission and took his photograph.⁸⁰ All three members of the Court of Appeal encouraged the development of legislation that would protect the privacy of a person in these circumstances.⁸¹
- 7.36 In *Campbell* Lord Nicholls referred to this issue when he observed that an ‘individual’s privacy can be invaded in ways not involving publication of information’ and that ‘strip searches are an example’.⁸² This is what happened in *Wainwright v Home Office*, in which a woman and her son were strip searched before being permitted to visit a family member in prison.⁸³ The House of Lords found that the common law had no remedy for them even though the prison officers did not have any statutory authority to conduct the strip searches. In this case the court was unable to fill any ‘perceived gap’ in the law by ‘judicious development of an existing principle’.⁸⁴

THE LAW IN NEW ZEALAND

A tort of invasion of privacy by publishing private facts

- 7.37 The New Zealand courts have developed a tort of breach of privacy by giving publicity to private and personal information.⁸⁵ The tort concerns conduct that is similar to that which falls within the UK extended cause of action for breach of confidence by misuse of private information. Despite this similarity, the majority of the New Zealand Court of Appeal chose to acknowledge the existence of a new tort rather than follow the approach of the UK courts. They did this in order to ‘allow the law to develop with a direct focus on the legitimate protection of privacy, without the need to be related to issues of trust and confidence’.⁸⁶ The majority judges observed that as privacy and confidence are different concepts, it could be confusing to ‘press every case calling for a remedy for unwarranted exposure of information about the private lives of individuals into a cause of action having as its foundation trust and confidence’.⁸⁷

7.38 The majority judges said that it is up to the legislature to develop ‘any high-level and wide tort of invasion of privacy’.⁸⁸ In developing the new tort the majority referred to New Zealand’s international human rights obligations and observed that the ‘intrusiveness of the long-range lens and listening devices and the willingness to pay for and publish the salacious are factors in modern society of which the law must take account’.⁸⁹ They went on to say that it is ‘the very process of the common law’ for the courts to devise new civil remedies in response to these developments.⁹⁰

Elements

7.39 The elements of this new tort of invasion of privacy by publicising private information are

- the existence of facts in respect of which there is a reasonable expectation of privacy
- publicity given to those private facts that would be considered highly offensive to a reasonable person.⁹¹

7.40 In *Hosking v Runting*⁹² the New Zealand Court of Appeal concluded that these elements 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 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 that a person of ordinary sensibilities would find highly offensive or objectionable.⁹³ The court held that the photographs only disclosed what any member of the public in that area could see on the particular day, and there was no harm in publication of the photographs, even though they were of children.⁹⁴

7.41 The second element of the New Zealand tort—that the publicity given to private facts is highly offensive to a reasonable person—is not found in the UK action for breach of confidence. The majority judges in *Hosking v Runting* explained the reasoning that led to the adoption of this test drawn from US privacy law. After acknowledging that people give up expectations of complete privacy and seclusion by living in communities, they said they were concerned with ‘widespread publicity of very personal and private matters’ which is ‘truly humiliating and distressful or otherwise harmful to the individual concerned’.⁹⁵

7.42 The result in *Hosking v Runting* is different to that reached in a very similar recent UK case involving the publication of photographs of the infant son of noted children’s author J K Rowling, taken by a professional photographer with a long-range lens.⁹⁶ The two courts reached different conclusions about whether there was a reasonable expectation of privacy in relation to photographs of a child of a celebrity taken in a public street. The English Court of Appeal held that J K Rowling’s action on behalf of her son should be permitted to proceed⁹⁷ because

*the law should ... protect children from intrusive media attention, at any rate to the extent of holding that a child has a reasonable expectation that he or she will not be targeted in order to obtain photographs in a public place for publication which the person who took or procured the taking of the photographs knew would be objected to on behalf of the child.*⁹⁸

77 *OBG Ltd v Allan* [2008] 1 AC 1 [255] (Lord Nicholls).

78 *OBG Ltd v Allan* [2008] 1 AC 1 [292].

79 See [7.55–7.62].

80 *Kaye v Robertson* [1991] FSR 62.

81 *Kaye v Robertson* [1991] FSR 62, 66 (Glidevwell LJ), 70 (Bingham LJ), 71 (Leggatt LJ).

82 *Campbell v MGN Ltd* [2004] 2 AC 457 [15].

83 *Wainwright v Home Office* [2004] 2 AC 406.

84 *Wainwright v Home Office* [2004] 2 AC 406 [18] (Lord Hoffmann).

85 *Hosking v Runting* [2005] 1 NZLR 1.

86 *Hosking v Runting* [2005] 1 NZLR 1[148] (Gault P and Blanchard J); Tipping J expressed general agreement with Gault P and Blanchard J [223].

87 *Hosking v Runting* [2005] 1 NZLR 1[48] (Gault P and Blanchard J).

88 *Hosking v Runting* [2005] 1 NZLR 1[110] (Gault P and Blanchard J).

89 *Hosking v Runting* [2005] 1 NZLR 1[109] (Gault P and Blanchard J).

90 *Hosking v Runting* [2005] 1 NZLR 1[109] (Gault P and Blanchard J).

91 *Hosking v Runting* [2005] 1 NZLR 1 [117] (Gault P and Blanchard J).

92 [2005] 1 NZLR 1.

93 *Hosking v Runting* [2005] 1 NZLR 1 [164]–[165].

94 *Hosking v Runting* [2005] 1 NZLR 1 [164]–[165].

95 *Hosking v Runting* [2005] 1 NZLR 1[125]–[126] (Gault P and Blanchard J).

96 *Murray v Big Pictures (UK) Limited* [2008] EWCA Civ 446.

97 The case was an appeal against a decision by the trial judge to strike out the proceedings because the pleaded facts did not disclose a cause of action. The Court of Appeal overturned that decision and directed the case proceed to trial.

98 *Murray v Big Pictures (UK) Limited* [2008] EWCA Civ 446 [57].

Defences

- 7.43 The majority judges in *Hosking v Runting* suggested that there should be a defence of legitimate public concern in order to ensure that ‘the scope of privacy protection should not exceed such limits on the freedom of expression as is justified in a free and democratic society’.⁹⁹ They used the term ‘public concern’ rather than public interest to differentiate ‘matters of general interest or curiosity to the public, and matters which are of legitimate public concern’.¹⁰⁰ They acknowledged that this might require judges to balance interests by considering ‘community norms, values and standards’.¹⁰¹
- 7.44 Although the New Zealand courts have had few opportunities to develop the defences to this new cause of action, the New Zealand Law Commission has suggested that consent should be a defence, as it is to all torts.¹⁰² The Commission has also pointed out that it should be possible to rely upon a defence that an act was privileged, or performed under legal authority, if it did not fall within the broad defence of legitimate public concern identified in *Hosking v Runting*.¹⁰³

Remedies

- 7.45 The majority judges said that the ‘primary remedy upon a successful claim will be an award of damages’ and that ‘injunctive relief may be appropriate in some circumstances’.¹⁰⁴ They said actual damage in the sense of ‘personal injury or economic loss’ is unnecessary and that the ‘harm to be protected against is in the nature of humiliation and distress’.¹⁰⁵ Proof of recognised psychiatric harm is unnecessary.¹⁰⁶
- 7.46 When dealing with the availability of injunctive relief, the majority judges acknowledged legitimate concerns about ‘prior restraint’ of material the media wish to publish.¹⁰⁷ They suggested an injunction should not be granted to restrain publication unless there is ‘compelling evidence of most highly offensive intended publicising of private information and there is little legitimate public concern in the information’.¹⁰⁸

Comment

- 7.47 The precise status of the New Zealand tort of invasion of privacy by publishing private facts is uncertain because some members of the country’s new highest court, the Supreme Court, have cast doubts upon its continued acceptance and its content. In a recent case¹⁰⁹ Justice Anderson, who was one of the two dissenting judges in *Hosking v Runting*,¹¹⁰ said that, in his view, the existence of the tort and its scope were matters for debate in the Supreme Court.¹¹¹ Chief Justice Elias queried the details of the tort, particularly the need for the second element concerning the ‘highly offensive’ nature of the publicity.¹¹²
- 7.48 There have been relatively few cases in New Zealand dealing with the tort of invasion of privacy by publishing private facts since developments started at the trial court level in the mid 1980s. It appears that ‘fifteen people have brought cases wholly or partly based on privacy, and many of them have been neither rich nor famous’.¹¹³ The New Zealand Law Commission has published brief details of all of these cases.¹¹⁴ Damages were ordered in only two cases, with the highest award being NZ\$25 000.¹¹⁵ An injunction restraining publication was granted on five occasions.¹¹⁶

7.49 The New Zealand Law Commission has recently recommended that development of the tort recognised in *Hosking v Runting* should be left to the common law.¹¹⁷ Although the Commission acknowledged that a statutory cause of action would make the law more accessible and certain, it referred to the absence of ‘evidence that the current state of the law is causing practical difficulties to anyone’.¹¹⁸

Intrusion upon seclusion

7.50 The majority of the Court of Appeal in *Hosking v Runting*¹¹⁹ said that they were dealing with only one of the four strands of the US privacy tort¹²⁰—wrongful publicity given to private lives—and that the scope of the cause of action should be left to incremental development by the courts. They stated that it was unnecessary to decide ‘whether a tortious remedy should be available ... for unreasonable intrusion into a person’s solitude or seclusion’.¹²¹

7.51 In its Issues Paper, the New Zealand Law Commission argued for the introduction of a separate intrusion upon seclusion tort, suggesting that some intrusions upon spatial privacy may be regarded as unacceptable invasions of privacy, regardless of whether they are accompanied by unwanted disclosure of private information.¹²²

7.52 The New Zealand Law Commission ultimately recommended that any recognition and development of a tort of intrusion into seclusion should be left to the common law.¹²³ The Commission concluded that ‘the development of such a tort deserves serious consideration’ and said that the ‘real question is whether it should be introduced by statute, or whether it should be left to develop at common law’.¹²⁴ Because of its support for the common law tort of invasion of privacy by publishing private facts, the Commission was content to leave development of an intrusion tort to the courts.¹²⁵

THE LAW IN THE UNITED STATES

7.53 Nearly all US states now recognise a right to privacy, either at common law or, in a few states, as a creation of statute.¹²⁶ There are four types of invasion of privacy:

- intrusion of seclusion
- appropriation of name or likeness
- publicity given to private life
- publicity placing a person in a false light.¹²⁷

7.54 Although most plaintiffs in privacy cases rely on more than one of the privacy torts,¹²⁸ the two causes of action most relevant to surveillance are intrusion upon the seclusion of, and publicity given to, private life. These are also the two privacy torts most concerned with ‘the fundamental value of personal autonomy’.¹²⁹

Tort of intrusion upon seclusion

Elements

7.55 According to the Restatements of the Law, published to give judges greater clarity about the law, ‘one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of privacy, if the intrusion would be highly offensive to a reasonable person’.¹³⁰ The tort includes physical intrusions, as well as ‘sensory intrusions such as eavesdropping, wiretapping, and visual and photographic spying’.¹³¹

- 99 *Hosking v Runting* [2005] 1 NZLR 1[129]–[130] (Gault P and Blanchard J).
- 100 *Hosking v Runting* [2005] 1 NZLR 1[133] (Gault P and Blanchard J).
- 101 *Hosking v Runting* [2005] 1 NZLR 1[135] (Gault P and Blanchard J).
- 102 New Zealand Law Commission, *Invasion of Privacy: Penalties and Remedies Stage 3 Report* No 113 [6.91].
- 103 *Ibid.*
- 104 *Hosking v Runting* [2005] 1 NZLR 1[149] (Gault P and Blanchard J).
- 105 *Hosking v Runting* [2005] 1 NZLR 1[135] (Gault P and Blanchard J).
- 106 *Ibid.*
- 107 *Hosking v Runting* [2005] 1 NZLR 1[151] (Gault P and Blanchard J).
- 108 *Hosking v Runting* [2005] 1 NZLR 1[158] (Gault P and Blanchard J).
- 109 *Rogers v Television New Zealand Ltd* [2008] 2 NZLR 277 (SC).
- 110 [2005] 1 NZLR 1.
- 111 *Rogers v Television New Zealand Ltd* [2008] 2 NZLR 277 [144] (SC).
- 112 *Rogers v Television New Zealand Ltd* [2008] 2 NZLR 277 [25] (SC).
- 113 Professor John Burrows, ‘Privacy and the Courts’ (Address to the Privacy Forum, Wellington New Zealand, 27 August 2008) <www.privacy.org.nz/assets/Files/PAW/10.-Speaker-Professor-John-Burrows.doc> at 10 November 2009.
- 114 New Zealand Law Commission, above n 72, 158–160.
- 115 *Brown v Attorney-General* [2006] DCR 630.
- 116 New Zealand Law Commission above n 72.
- 117 New Zealand Law Commission, above n 102, 91.
- 118 *Ibid.* 90.
- 119 [2005] 1 NZLR 1.
- 120 See [7.55–7.69] for a discussion of the US privacy tort.
- 121 *Hosking v Runting* [2005] 1 NZLR 1[118] (Gault P and Blanchard J).
- 122 New Zealand Law Commission, above n 72 [1.2].
- 123 New Zealand Law Commission, above n 102, 93.
- 124 *Ibid.* 92.
- 125 *Ibid.* 93.
- 126 W Page Keeton et al (eds) *Prosser and Keeton on the Law of Torts* (5th ed) (1984) 851 with reference to statutes in New York, Utah, Virginia, Wisconsin, and Nebraska.
- 127 William Prosser, ‘Privacy’ (1960) 48 (3) *California Law Review* 383, 388–389.
- 128 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, 1008.
- 129 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199 [125] (Gummow and Hayne JJ) citing Sedley LJ in *Douglas v Hello! Ltd* [2001] QB 967 at 1001.
- 130 Restatement (Second) of Torts § 652B (1977).
- 131 *Ruth Shulman v Group W Productions* (1998) 18 Cal 4th 200, 230–231; 955 P2d 469, 489; 74 Cal Rptr 2d 843, 863 citing Restatement (Second) of Torts § 652B cmt b (1977).

7.56 The tort has two elements:

- intrusion into a private place, conversation or matter; and
- in a manner highly offensive to a reasonable person.¹³²

7.57 The requirement that the intrusion upon seclusion be ‘highly offensive to a reasonable person’ means that the interference with seclusion must be substantial and involve conduct that would elicit strong objection from a reasonable person.¹³³ An often-cited example is a press photographer who enters the hospital room of a woman who has a rare illness and takes her photograph, even though she previously objected to giving an interview.¹³⁴

7.58 The intrusion itself subjects the defendant to liability, regardless of whether he or she has published information gained from the intrusion.¹³⁵ According to Andrew McClurg: ‘this is important because it insulates the tort of intrusion from many of the free speech obstacles that infiltrate the other privacy torts, most notably the tort of public disclosure of private facts’.¹³⁶

7.59 The US Supreme Court has held that the First Amendment to the US Constitution prohibits actions for invasion of privacy where the published matter is truthful and lawfully obtained information of legitimate public concern.¹³⁷ By contrast, the US Constitution provides only a limited right to gather information, which is the right more directly implicated by intrusions into seclusion.¹³⁸ Further, because the ‘public interest test’ does not apply in the tort of intrusion, ‘it is technically irrelevant whether the subject of intrusion is a public figure and/or whether information acquired during the intrusion is a matter of public interest’.¹³⁹

Application in public places

7.60 The tort of intrusion has been of limited use to people whose privacy has been invaded in public places. This is due to what has been described as the ‘stubborn principle’ in US tort law that privacy cannot be invaded in or from a public place.¹⁴⁰ William Prosser wrote in his 1960 article:

*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.*¹⁴¹

7.61 The principle also appears in the Restatements, which adopted his view that the tort of intrusion generally cannot occur in public places.¹⁴² According to the Restatements, there is no ‘liability for observing ... or even taking [a plaintiff’s] photograph while he is walking on the public highway, since he is not then in seclusion, and his appearance is public and open to the public eye’.¹⁴³

7.62 The Restatements acknowledges a narrow exception to the rule where the intrusion concerns a matter that is not normally exhibited to the public gaze, such as details of a person’s undergarments.¹⁴⁴ Similarly, there may be privacy in public with respect to a matter that is very personal in nature or implicates a person’s ‘emotional sanctum’.¹⁴⁵ A number of cases have also said unreasonable, harassing or persistent surveillance of individuals in public places can be unlawful.¹⁴⁶

Tort of publicity given to private life

Elements

7.63 The Restatements defines the tort of publicity given to private life in the following terms:

One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of privacy, if the matter publicized is of a kind that

- *would be highly offensive to a reasonable person, and*
- *is not of legitimate concern to the public.*¹⁴⁷

7.64 Thus, like the tort of intrusion upon seclusion, the tort of publicity given to private life requires that the information publicised is highly offensive to a reasonable person.¹⁴⁸ In contrast to the tort of unreasonable intrusion, however, publication is a necessary element of the tort of unreasonable publicity.

7.65 The further requirement that the matter publicised is not of legitimate concern to the public stems from concerns with freedom of the press, and the privilege under the common law to giving publicity to news, and other matters of public interest.¹⁴⁹ According to the Restatements, 'when the matter to which publicity is given is true, it is not enough that the publicity would be highly offensive to a reasonable person'.¹⁵⁰ The US Supreme Court has found that the First Amendment to the US Constitution prohibits actions for invasion of privacy where the matter publicised is truthful and was lawfully obtained.¹⁵¹

Application in public places

7.66 Like the tort of seclusion, the tort of publicity is generally not available when the information in question was gathered in a public place. According to the Restatements

*there is no liability for giving further publicity to what the plaintiff himself leaves open to the public eye. Thus he normally cannot complain when his photograph is taken while he is walking down the public street and is published in the defendant's newspaper.*¹⁵²

Defences

7.67 Leading commentators suggest that consent may be the only defence in actions for invasion of privacy.¹⁵³ Consent may not in fact be a true defence because one element of the tort—an offensive invasion of privacy—could not be established if the plaintiff had consented to the conduct in question.¹⁵⁴

Remedies

7.68 In the US, a successful claim of invasion of privacy under common law entitles the plaintiff to recover damages on three bases:

- the harm from the loss of privacy
- mental distress reasonably suffered
- when there is cause for 'special damages'.¹⁵⁵

7.69 It remains unclear whether damages can be awarded in the absence of proof of actual harm.¹⁵⁶ Injunctions are not readily ordered.¹⁵⁷

132 *Ruth Shulman v Group W Productions* (1998) 18 Cal 4th 200, 231; 955 P2d 469, 490; 74 Cal Rptr 2d 843, 864.

133 Restatement (Second) of Torts § 652B cmt d (1977).

134 Restatement (Second) of Torts § 652B cmt b, illus 1 (1977).

135 Restatement (Second) of Torts § 652B cmts a–b (1977).

136 McClurg, above n 128, 1070.

137 *Cox Broadcasting Co v Cohn*, 420 US 469 (1975); *The Florida Star v BIF*, 491 US 524 (1989).

138 McClurg, above n 128, 1070–1.

139 *Ibid* 1078–1079.

140 *Ibid* 999.

141 Prosser, above n 127, 391–2.

142 McClurg, above n 128, 1026.

143 Restatement (Second) of Torts § 652B cmt c (1977).

144 Restatement (Second) of Torts § 652B cmt c (1977).

145 *Harvey Martin and David Whitten v Robert Patterson, individually, and d/b/a Patterson Construction* (2007) 975 So 2d 984, 994.

146 See eg, *Galella v Onassis*, 487 F2d 986 (2nd Cir, 1973); *Nader v General Motors Corporation*, 255 NE 2d 765 (NY Ct App 1970); Robert Gellman, 'A General Survey of Video Surveillance in the United States' in Sjaak Nouwt et al (eds) *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy* (2005), 7, 32 citing Annotation, 'Right of Privacy—Surveillance', 13 ALR 3rd (1967) 1025, 1026.

147 Restatement (Second) of Torts § 652D (1977).

148 Keeton, above n 126, 857.

149 *Ibid* 860.

150 Restatement (Second) of Torts § 652D cmt d (1977).

151 *Cox Broadcasting Co v Cohn* 420 US 469 (1975); *The Florida Star v BIF* (1989) 491 US 524, 541.

152 Restatement (Second) of Torts § 652D cmt b (1977).

153 Keeton, above n 126, 868.

154 *Ibid* 867.

155 Restatement (Second) of Torts § 652H (1977).

156 Restatement (Second) of Torts § 652H (1977).

157 Robert Gellman, 'A General Survey of Video Surveillance in the United States', in Sjaak Nouwt et al (eds) *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy* (2005) 7, 34.

THE LAW IN CANADA**Statutory causes of action for invasion of privacy**

7.70 There is no common law tort of invasion of privacy in Canada.¹⁵⁸ However, four provinces—British Columbia, Manitoba, Saskatchewan, and Newfoundland and Labrador—have statutory causes of action for invasion of privacy.¹⁵⁹ British Columbia enacted the first Privacy Act in 1968, followed by Manitoba (1970), Saskatchewan (1974), and Newfoundland and Labrador (1981).¹⁶⁰

Elements of the statutory causes of action

- 7.71 All of the provincial statutes create broadly defined causes of action. In British Columbia, for example, it is a tort, without proof of damage, ‘for a person, wilfully and without claim of right to violate the privacy of another’.¹⁶¹
- 7.72 The elements of the statutory causes of action are similar. First, the plaintiff’s expectation of privacy must be reasonable. For example, the British Columbia Act provides that ‘the nature and degree of privacy to which a person is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, giving due regard to the lawful interests of others’.¹⁶² Among the factors the courts look at to determine reasonableness is the location of the privacy invasion and, in the case of surveillance, whether it was conspicuous, together with its extent, thoroughness and duration.¹⁶³
- 7.73 Secondly, all but the Manitoba Act require proof that the defendant acted wilfully. This means that the defendant knew, or ought to have known, that an act would violate the privacy of the plaintiff, and was not merely negligent.¹⁶⁴
- 7.74 Thirdly, the statutes require the courts to consider a range of relevant factors such as the nature of the privacy invasion and the relationship between the parties. With the exception of the Manitoba Privacy Act, which stipulates that an invasion of privacy must be ‘substantial’, the legislation does not require the alleged invasion of privacy to be ‘serious’ or ‘highly offensive’.¹⁶⁵
- 7.75 The Canadian provincial statutes include three of the four US privacy torts. Cases brought under these laws have found liability for intrusion into seclusion and disclosure of embarrassing private facts. The Canadian Acts also explicitly provide for a right of action for misappropriation of personality.¹⁶⁶

Defences

- 7.76 All four Acts list exceptions or defences to the cause of action. The common exceptions or defences are:
- the plaintiff consented to the conduct
 - the defendant’s conduct was incidental to the exercise of a lawful right of defence of person or property
 - the defendant’s conduct was authorised or required by law
 - the defendant is a police or public officer who was engaged in his/her duty and the conduct was neither disproportionate to the matter being investigated nor committed in the course of a trespass
 - if the defendant’s conduct involved publication, the publication was privileged, fair comment or was in the public interest.

7.77 The Saskatchewan Privacy Act also contains a defence of acting in the scope of newsgathering, while the Manitoba Act has a defence for a person who neither knows, nor reasonably should have known, that the act in question would violate the privacy of any person.

Remedies

7.78 The Canadian statutes, other than the British Columbia Privacy Act, specify the remedies that a court may order for an unlawful invasion of privacy. Common remedies are:

- damages
- an injunction
- an order for the defendant to account to the plaintiff for profits in consequence of the violation
- an order for the defendant to deliver the documents obtained in consequence of the violation.

7.79 In British Columbia, damages are the only remedy that has been ordered by the courts.¹⁶⁷

Comment

7.80 There have been relatively few privacy cases in Canada. By 2001, there had been no more than 25 privacy cases under the four provincial statutes.¹⁶⁸ Most of those cases had been taken under the British Columbia Privacy Act.¹⁶⁹

7.81 The small number of cases may be due in part to the cost of litigation. For example, in British Columbia, jurisdiction is vested solely in the Supreme Court, where the high cost of bringing an action is a disincentive to litigation.¹⁷⁰

OTHER LAW REFORM COMMISSION RECOMMENDATIONS

AUSTRALIAN LAW REFORM COMMISSION

7.82 The ALRC proposed a new statutory cause of action for serious invasion of privacy in its report about protection of privacy in Australia.¹⁷¹ When the Australian Government announced its intention to implement many of the ALRC's recommendations in a document published in October 2009, it indicated it would not respond to the recommendations concerning a new cause of action until an unspecified later date.¹⁷²

7.83 The ALRC recommended a broad statutory cause of action for serious invasion of privacy.¹⁷³ Although the ALRC did not seek to define 'serious invasion of privacy', it did provide a non-exhaustive list of the circumstances that could give rise to the cause of action. They were:

- if there has been an interference with an individual's home or family life
- if an individual has been subjected to unauthorised surveillance
- if an individual's correspondence or private written, oral or electronic communication has been interfered with, misused or disclosed
- if sensitive facts relating to an individual's private life have been disclosed.¹⁷⁴

158 Neither the Supreme Court of Canada nor any provincial courts of appeal have endorsed a common law tort of invasion of privacy: Colin McNair and Alexander Scott, *Privacy Law in Canada* (2001) 45; Simon Chester, Jason Murphy and Eric Robb, 'Zapping the Paparazzi: Is the Tort of Privacy Alive and Well?' (2003) 27 *Advocates Quarterly* 357, 360. However, some lower courts have been prepared to do so. See eg, *Somwar v MacDonald's Restaurants of Canada Ltd* [2006] OJ No 64 as discussed in Alex Cameron and Mimi Palmer, 'Invasion of Privacy as a Common Law Tort in Canada' (2009) 6(11) *Canadian Privacy Law Review* 105.

159 *Privacy Act*, RSBC 1996, c 373, *Privacy Act*, RSM 1987, c P125, *Privacy Act*, RSS 1978, c P-24, *Privacy Act*, RSNL 1990, c P-22. The province of Quebec, which is a civil rather than a common law jurisdiction, has also enacted a statutory cause of action for invasion of privacy. McNair, above n 158, 66, citing Articles 35-40 of the Civil Code of Quebec, SQ 1991, c 64.

160 McNair, above n 158, 68, 70, 72.

161 *Privacy Act*, RSBC 1996, c 373, s 1(1).

162 *Privacy Act*, RSBC 1996, c 373, s 1(2).

163 McNair, above n 158, 79 citing *Davis v McArthur* (1969) 10 DLR (3d) 250 (BCSC).

164 British Columbia Law Institute, *Report on the Privacy Act of British Columbia* BCLI Report No 49 (2008) 11 citing *Hollinsworth v BCTV* (1998) 59 BCLR (3d) 121 (CA) and *Getejanc v Brentwood College Association* (2001) 6 CCLT (3d) 261 at [22] (BCSC).

165 McNair, above n 158, 67.

166 *Ibid* 76.

167 British Columbia Law Institute, above n 164, 40-1.

168 McNair, above n 158, 73.

169 Chester, above n 158, 364.

170 McNair, above n 158, 70.

171 Australian Law Reform Commission, above n 2, 19.

172 Australian Government, *Australian Government First Stage response to the ALRC Report 108* (2009).

173 Australian Law Reform Commission, above n 2, rec 74-1.

174 Australian Law Reform Commission, above n 2 [74.119]. It appears that 'unauthorised surveillance' is surveillance not authorised by any law. This description probably includes most surveillance that currently takes place in Victoria.

7.84 The ALRC concluded that a statutory cause of action was ‘the best way’ to protect people from ‘unwanted intrusions into their private lives or affairs in a broad range of contexts’.¹⁷⁵ It supported legislative intervention because of concern about ‘a lengthy period of uncertainty and inconsistency as the courts refine the law in this area’.¹⁷⁶ The ALRC suggested that a statutory cause of action would overcome ‘the distinction between equitable and tortious causes of action, and between the defences and remedies available under each’.¹⁷⁷

Elements of the cause of action

7.85 The ALRC recommended that the elements of the cause of action should be that

- the claimant had a reasonable expectation of privacy in the circumstances
- the act or conduct complained of is highly offensive to a reasonable person of ordinary sensibilities.¹⁷⁸

These elements are similar to those adopted by the New Zealand Court of Appeal when devising the tort of misuse of private information. The ALRC cause of action, however, extends to a much broader range of activities because it seeks to deal with a serious invasion of privacy in any circumstances.

7.86 The ALRC proposed that a court undertake a balancing of interests when considering the two elements of the cause of action. The court would be required to consider whether ‘the public interest in maintaining the claimant’s privacy’ outweighs ‘other matters of public interest’, such as being informed about matters of public concern and freedom of expression.¹⁷⁹ This balancing exercise, which is very similar to the second element of the UK cause of action for misuse of private information,¹⁸⁰ requires the court to consider those ‘other matters of public interest’ when considering both elements of the cause of action.

7.87 The ALRC argued that including the public interest test within the elements of the cause of action recognises the importance of freedom of expression. If freedom of expression were merely a defence, claims without merit could proceed with defendants having to wait until the defence case to raise their public interest defence.¹⁸¹

7.88 The ALRC’s recommended cause of action requires conduct that is either deliberate or reckless, and not merely negligent. Negligent acts were excluded because ‘including liability for negligent or accidental acts in relation to all invasions of privacy would, arguably, go too far’.¹⁸²

Defences

7.89 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.¹⁸³

7.90 The ALRC suggested that defences that are commonly recognised in other countries—such as consent, information in the public domain, and disclosure to rebut an untruth—are subsumed within the elements of the cause of action. For example, a person who consented to a particular course of conduct could not have a reasonable expectation of privacy and nor could the defendant’s actions be highly offensive to an ordinary person of reasonable sensibilities.¹⁸⁴

Remedies

7.91 The ALRC's proposed cause of action does not require proof of actual damage. This means that proof of physical or economic harm is unnecessary and that the cause of action extends to conduct that causes insult or humiliation. 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. Although the ALRC did not directly address the matter, it seems apparent that the Federal Court and the Federal Magistrates Court would exercise jurisdiction in these cases.

NSW LAW REFORM COMMISSION

7.92 In 2009 the NSWLRC recommended a statutory cause of action for invasion of privacy.¹⁸⁵ Like the ALRC, the NSWLRC recommended that it be a broad cause of action for 'invasion of privacy' generally. Although declining to define 'privacy', the NSWLRC said that its proposed cause of action seeks to protect two interests: invasions of information privacy and intrusions on seclusion.¹⁸⁶ It suggests that the courts will develop and refine the cause of action over time.¹⁸⁷ Unlike the ALRC, it did not limit the cause of action to serious invasions of privacy.

Elements of the cause of action

7.93 There are two elements to the NSWLRC's proposed cause of action.¹⁸⁸ The first element is that the individual concerned (P) had a reasonable expectation of privacy in the circumstances having regard to any relevant public interest and that P's privacy was invaded by the conduct of the alleged wrongdoer (D).¹⁸⁹ It is also necessary for P to prove, as a second element, that he or she did not consent to the conduct in question.

7.94 The NSWLRC rejected the second element in the ALRC's model cause of action—that the act or conduct complained of is highly offensive to a reasonable person of ordinary sensibilities—because it concluded that it is 'unwarranted in principle'.¹⁹⁰ The NSWLRC said that the 'highly offensive' test amounts to a qualification of the 'reasonable expectation of privacy test' which would unnecessarily privilege other interests, such as freedom of expression, over protection of privacy.¹⁹¹

7.95 The NSWLRC recommended that in order to balance P's interests with any other relevant interests, a court should be legislatively required to consider nine matters when deciding whether there has been an invasion of privacy. Those matters are:

- the nature of the subject matter alleged to be private
- the nature of the conduct concerned, including the extent to which a person of ordinary sensibilities would consider the conduct offensive
- the relationship between P and D
- the extent to which P has a public profile
- the extent to which P was in a position of vulnerability
- the conduct of P and D before and after the event, including any apology by D
- the effect of D's conduct on P's health and welfare
- whether D's conduct contravened any Australian statute
- any other matter the court considers relevant.¹⁹²

175 Australian Law Reform Commission, above n 2 [74.117].

176 Ibid.

177 Ibid.

178 Ibid rec 74–2.

179 Ibid rec 74–2.

180 See discussion at 7.16–7.33.

181 Australian Law Reform Commission, above n 2 [74.144], [74.147].

182 NSW Law Reform Commission, above n 6 [7.24].

183 Australian Law Reform Commission, above n 2 [74.169].

184 Ibid [74.174].

185 NSW Law Reform Commission, *Invasion of Privacy*, Report No 120, (2009).

186 Ibid 4.11.

187 Ibid 4.16.

188 The precise wording of the cause of action is set out in the draft legislation that the Commission prepared as part of its report. See NSW Law Reform Commission, above n 185, 80–92.

189 The requirement to balance competing interests that is built into the two elements in the ALRC model is made explicit in the NSW model.

190 NSW Law Reform Commission, above n 185 [5.11].

191 Ibid.

192 Ibid [5.21].

- 7.96 The NSWLRC suggested that the proposed cause of action should be characterised as a statutory action rather than as a tort for two reasons. First, it reasoned that the methodology of the cause of action is not that usually associated with torts because they 'do not generally require the courts to engage in an overt balancing of relevant interests ... in order to determine whether or not the elements of the cause of action in question are satisfied'. Secondly, it argued that the proposed cause of action 'should not necessarily be constrained by rules or principles generally applicable in the law of torts'.¹⁹³
- 7.97 The NSWLRC identified two tort rules or principles that were of concern: the state of mind of the wrongdoer and the extent to which actual damage forms part of the cause of action. If the cause of action were characterised as a tort it would be necessary to determine whether the wrongdoer's conduct was intentional in order to attract liability. Although the Commission was of the view that liability should generally arise only where the conduct in question was intentional, it preferred to leave the matter to the courts because there might be circumstances in which a person should be held liable for reckless or negligent conduct, such as when a doctor negligently discloses medical records. If the cause of action were characterised as a tort it would also be necessary to determine whether it was a tort that is actionable without proof of damage, such as trespass, or whether actual proof of damage is necessary, as in the tort of negligence. The Commission was of the view that this requirement of tort law 'is inapposite to the statutory cause of action, which is designed primarily to protect the plaintiff from suffering non-economic loss, including mental distress'.¹⁹⁴

Defences

- 7.98 The NSWLRC recommended that there should be five statutory defences to the cause of action for invasion of privacy. These defences are similar to those found in the Canadian provinces that have statutory causes of action. The defendant bears the burden of proof in relation to the statutory defences, which are:
- D's conduct was required or authorised by law
 - D's conduct was done in lawful defence of a person or property
 - D's conduct involved publication of information in circumstances where under defamation law D could rely upon the defences of absolute privilege or fair reporting
 - D's conduct involved publication of information as an employee or agent of a subordinate distributor and D could not have reasonably known that the publication constituted an invasion of privacy
 - D's conduct involved publication of information in circumstances similar to those that attract the defence of qualified privilege in defamation law and D's conduct was not actuated by malice.¹⁹⁵
- 7.99 There are no public interest defences in the draft legislation prepared by the NSWLRC. Rather, in determining whether an individual's privacy has been invaded for the purposes of the action, a court must consider any relevant public interest, including the interest of the public in being informed about matters of public concern.¹⁹⁶

Remedies

7.100 The NSW Commission proposes that a court be permitted to order a range of statutory remedies, including compensatory damages, injunctive style prohibitory orders and orders of a declaratory nature. The draft legislation caps the amount of compensation that may be awarded for non-economic loss at \$150,000, with this maximum figure being adjusted on an annual basis. Exemplary or punitive damages are specifically excluded.

Jurisdiction

7.101 The NSWLRC proposed that the cause of action be created by state legislation as part of a uniform national law project. Jurisdiction should be vested in a state court of competent jurisdiction.

7.102 The cause of action is available only to living 'individuals' or natural persons. Any cause of action would not survive the death of the complainant. Proceedings must be commenced within 12 months of the date upon which the cause of action accrues unless a court extends that limitation period. Any extension cannot exceed three years from the date upon which the cause of action accrued.

SHOULD VICTORIA ENACT A CAUSE OF ACTION FOR INVASION OF PRIVACY?

7.103 In our Consultation Paper, we suggested that consideration be given to whether Victoria should have a statutory cause of action for serious invasions of privacy modelled on the recommendations in the ALRC's Privacy Report.¹⁹⁷

7.104 The commission received a range of views about the proposed cause of action. There was broad support for a statutory cause of action,¹⁹⁸ although it was carefully qualified in a number of instances.¹⁹⁹ A number of organisations also expressed direct opposition to the proposal.²⁰⁰

7.105 Support for a cause of action was often accompanied by the suggestion that it would fill a gap in the protection of privacy in Victoria. For example, some groups supported the cause of action because of its capacity to deal with once-off or intermittent use of surveillance by individuals where other forms of regulation might fail.²⁰¹ Others took a slightly broader view. The Victorian Privacy Commissioner, for example, wrote:

*A large number of individuals who contact the Office of the Victorian Privacy Commissioner ... seek redress for interferences with spatial or physical privacy for which there is currently no readily accessible remedy in Australian law, or seek to complain about interferences with personal information by other individuals, which are effectively beyond the jurisdiction of all current privacy regulators.*²⁰²

7.106 The Law Institute of Victoria noted that the protection afforded the right to privacy by section 13 of the *Charter of Human Rights and Responsibilities Act 2006* (the Charter) is limited because it 'does [not] give rise to a direct cause of action for invasions of privacy and it is limited to acts of public authorities'.²⁰³ A statutory cause of action might fill this gap.

193 Ibid [5.55].

194 Ibid [5.57].

195 Ibid 85–6.

196 Ibid 86.

197 Australian Law Reform Commission, above n 2, rec 74–1.

198 Submissions 2, 5, 7, 9, 12, 20, 27, 29, 33, 34, 35, 36, 37, 38, 40, 42, 44; Consultations 4, 5, 9, 27.

199 Submissions 27, 36, 38, 40, 42; Consultation 5.

200 Submissions 16, 19, 22, 25, 28.

201 Submission 29; Consultation 5. See also Submissions 5, 20.

202 Submission 29.

203 Submission 27.

7.107 In some instances, submissions expressed the view that the introduction of a statutory cause of action is preferable to waiting for the courts to develop the cause of action as part of the common law.²⁰⁴ For example, the Victorian Privacy Commissioner wrote:

Relying on the courts to recognise a cause of action for privacy may not be the best approach, given the inherent limitations associated with the courts only being able to consider particular matters brought before them by parties resourced to access justice at the requisite level. In addition, the courts would be limited by existing remedies developed within the common law or equity.

*Legislators have a better opportunity to craft a cause of action that is more precisely targeted and which takes into account competing public interests. Moreover, protection of a fundamental human right such as privacy should not be dependent on the efforts of a particularly persistent and well resourced plaintiff, to take an action all the way to the High Court of Australia in order to definitively establish the existence of a cause of action.*²⁰⁵

7.108 Similarly, the Law Institute of Victoria noted that the evolution of common law protection for privacy was ‘too slow and too limited’ to provide protection from new surveillance technologies and other pressures on privacy protection such as counter-terrorism.²⁰⁶

7.109 A number of submissions referred to the limited capacity of a cause of action for serious invasions of privacy to control misuse of public place surveillance, especially when compared to other regulatory measures.²⁰⁷ The Fitzroy Legal Service, for example, acknowledged that a cause of action for serious invasions of privacy could protect the rights of individuals, but also noted that it would not address systemic discrimination, racial profiling, or harassment in the context of surveillance in public places.²⁰⁸

7.110 The capacity of the proposed statutory cause of action to be useful to the average person was questioned by some people. Some expressed concern that the cause of action would probably assist only those individuals able to afford the high cost of litigation.²⁰⁹ On the other hand, several people suggested that judicial consideration of the cause of action would set useful precedents for the entire community even if proceedings were taken only by the wealthy.²¹⁰ It was suggested that a high profile case would send an educative message about acceptable use of surveillance in public places.²¹¹

7.111 Although there was considerable support for a statutory cause of action, some organisations opposed the proposal that there be a cause of action for serious invasions of privacy.²¹² For example, some noted that a cause of action for invasion of privacy is best established at the federal level.²¹³ One submission suggested that the cause of action would alter the balance between privacy and competing rights, including freedom of communication.²¹⁴ Other organisations said that the introduction of a statutory cause of action is ‘excessive’,²¹⁵ and that current regulation of the media sufficiently protects any potential infringement of an individual’s privacy.²¹⁶

7.112 The federal Privacy Commissioner, who supports development of a statutory cause of action for invasion of privacy, encouraged ‘national consistency in the regulation of surveillance’ and ‘ongoing collaboration between governments to propose a cause of action that could be uniformly applied across all jurisdictions’.²¹⁷

THE COMMISSION'S RECOMMENDATION: TWO STATUTORY CAUSES OF ACTION

- 7.113 The commission is of the view that Victorians should be able to take civil action in response to threatened or actual serious invasions of privacy by the use of surveillance in a public place. Privacy is a value of increasing importance to the entire community because it recognises and promotes human dignity. The preamble to the Charter acknowledges that 'all people are born free and equal in dignity and rights'.
- 7.114 The reach of current privacy law is limited. There are Commonwealth and state laws that regulate how public authorities and some larger businesses deal with matters concerning information privacy. The *Surveillance Devices Act 1999* (Vic) (SDA) and the *Summary Offences Act 1966* (Vic) regulate the most flagrant invasions of privacy by use of a surveillance device. The extent to which the common law protects privacy is unclear.
- 7.115 Although the commission believes the introduction of proper guidelines, coupled with appropriate education about their implementation, will be an effective means of promoting responsible use of public place surveillance, new civil causes of action are warranted because, inevitably, some people will choose not to follow the guidelines. The possibility of civil action 'can create a climate of restraint which ensures that serious breaches do not happen in the first place', and can provide a unique response in particularly serious cases which require 'an injunction to stop an offensive publication happening in the first place'.²¹⁸
- 7.116 There is a clear gap in the current regulatory regime. Although the criminal law deals with the most offensive invasions of privacy, there is no parallel civil cause of action for people harmed by that behaviour. There is also no right of action for serious misuse of a surveillance device that falls short of criminal conduct. The Victorian Privacy Commissioner informed the commission that people contact her office with complaints about interferences with spatial privacy or misuse of private information for which for there is no redress under Victorian and Commonwealth law.
- 7.117 Events in other comparable countries suggest that the courts will face increasing pressure to develop a response to misuse of surveillance devices in a public place unless there is appropriate legislation. The developments in other common law countries, most notably the UK and New Zealand, suggest it will take a long time before a reasonably clear body of law emerges. Until that time, many people and organisations with a direct interest in the evolution of privacy causes of action will face substantial legal compliance costs to satisfy themselves that their proposed activities are lawful. The UK experience suggests a few pioneering plaintiffs, and some media organisations, will outlay significant sums of money in legal costs to develop the general law through the courts. This means of developing an important aspect of our law should be avoided if possible.
- 7.118 It is open to both the High Court and the Victorian Court of Appeal to recognise causes of action for wrongful publication of private information and for intrusion upon seclusion in the absence of any legislative action. This outcome could be achieved by following long recognised principles about the process by which the common law evolves. It is important to note that both the House of Lords and the New Zealand Court of Appeal were influenced by human rights principles when developing a cause of action for wrongful publication of private information.²¹⁹ The Victorian Court of Appeal may follow a similar course.²²⁰ That Court might be asked to consider what effect, if any, the right to privacy in the Victorian Charter²²¹ should have upon the common law as that body of law responds to changing social conditions.²²²

- 204 Submissions 27, 29.
205 Submission 29.
206 Submission 27.
207 Submissions 16, 19, 22, 25, 28.
208 Submission 34.
209 Consultation 5.
210 Submission 5; Consultation 5.
211 Consultation 5.
212 Submissions 19, 28.
213 Submissions 16, 21, 24.
214 Submission 28.
215 Submission 19.
216 Submission 28.
217 Submission 35.
218 John Burrows, 'Privacy and the Courts' (Address to the Privacy Forum, Hotel Intercontinental, Wellington, New Zealand, 27 August 2008) <www.privacy.org.nz/assets/Files/PAW/10.-Speaker-Professor-John-Burrows.doc > at 10 November 2009.
219 See *Campbell v MGN* [2004] 2 AC 457 [16]–[20] (Lord Nicholls), [49]–[50] (Lord Hoffmann); *Hosking v Runting* [2004] NZCA 34 [2]–[6] (Gault P and Blanchard J).
220 The remedies available in the general law action for breach of confidence were recently clarified by the Victorian Court of Appeal in *Giller v Procopets* [2008] 40 Fam LR 378. This decision is discussed in Robert Dean, 'Sex, Videotape and the Law' (2009) 83.08 *Law Institute Journal* 52.
221 *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 13.
222 While the Charter does not contain any express provision that directs the courts to consider human rights when developing the common law in light of changing social conditions (cf section 32 of the Charter, which deals with interpretation of statutory provisions), the courts could quite properly consider 'the human rights that Parliament specifically seeks to protect and promote' (section 7(1) of the Charter) when doing so.

- 7.119 Former High Court Chief Justice Sir Anthony Mason has suggested that a human rights charter guaranteeing a right to privacy 'could provide a platform for the development of a common law right'.²²³ Although the extent to which the High Court should, or may, consider the rights in the Victorian Charter when developing the Australian common law is a complex question, it can consider the right to privacy in international human rights instruments ratified by the Australian Government when doing so.²²⁴
- 7.120 The commission believes there should be two overlapping statutory causes of action for some serious invasions of privacy caused by misuse of a surveillance device in a public place. As national harmony of privacy law is likely to be a long-term goal, Victoria is well placed to demonstrate leadership in this area. The Charter is a useful catalyst for legislative action because 'privacy'²²⁵ is one of the human rights that 'Parliament specifically seeks to protect and promote'.²²⁶
- 7.121 The evidence from within Australia and other comparable countries suggests that there is unlikely to be a flood of litigation in response to the creation of any new causes of action for invasion of some privacy interests. There have been very few Australian cases in the eight years since the High Court indicated in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* that there were no common law barriers to the development of a cause of action for invasion of privacy.²²⁷ In New Zealand there have been approximately 15 privacy cases since 1985²²⁸ and Sir David Eady, the English High Court judge who has presided in some of the most significant privacy cases in that country, has recently written that after an early flurry of activity 'things seem to have settled down to a large extent'.²²⁹ He suggests this may mean 'that journalists and their lawyers have developed a feel for what is now acceptable to the general public (and to the courts) and what is not'.²³⁰
- 7.122 The commission believes that access to any causes of action for invasion of privacy should not be restricted to the few wealthy people who can afford the legal fees involved in court proceedings and have the financial capacity to accept the risk involved in any litigation. At the same time, senior judicial officers who have experience in weighing competing interests and shaping the law should hear the more difficult cases. The Victorian Civil and Administrative Tribunal (VCAT) is an ideal forum for these purposes because it is a low cost jurisdiction comprised of a broad range of judicial officers headed by a Supreme Court judge.
- 7.123 The commission believes it is not desirable for there to be one statutory cause of action for all serious invasions of privacy because the concept of privacy is too broad and imprecise to be of use when creating legal rights and obligations. Many appellate court judges and academic commentators have warned of the difficulty in devising a workable legal definition of privacy. In *Lenah Game Meats* Gleeson CJ said that 'the lack of precision of the concept of privacy is a reason for caution in declaring a new tort',²³¹ while Justices Gummow and Hayne referred to the 'difficulties in obtaining in this field something approaching definition rather than abstracted generalisation'.²³² Members of the House of Lords²³³ and the New Zealand Court of Appeal²³⁴ made similar comments when rejecting invitations to devise a broad tort of invasion of privacy.

- 7.124 Two internationally recognised academic commentators on privacy law, Daniel Solove and Raymond Wacks, make similar points. Solove suggests that while ‘privacy is an issue of profound importance around the world’,²³⁵ it is ‘a concept in disarray’ because ‘nobody can articulate what it means’.²³⁶ He argues that because ‘we should understand privacy as a set of protections against a plurality of distinct but related problems’²³⁷ it is advisable to identify particular types of privacy problems when considering regulation. Two of Solove’s privacy problem areas—information dissemination and invasion—are of particular relevance when considering new statutory causes of action involving misuse of surveillance devices. According to Solove, ‘*information dissemination* involves the transfer and publicizing of personal data’ and ‘*invasion* involves interference with one’s personal life’.²³⁸
- 7.125 Wacks suggests that one of the reasons why a tort of privacy has not evolved as part of the English common law is the lack of a coherent and consistent meaning of the notion of privacy.²³⁹ He argues that it is more constructive to identify the specific interests the law ought to protect and suggests that ‘at the core of the preoccupation with the “right to privacy” is protection against the misuse of personal, sensitive information’.²⁴⁰
- 7.126 The commission believes there should be two overlapping statutory causes of action concerning the privacy interests most likely to be adversely affected by the misuse of public place surveillance. Those causes of action should deal with misuse of private information and what is often referred to as intrusion upon seclusion, or unwarranted interference with spatial privacy. Legislating to protect these broadly recognised sub-categories of privacy is likely to promote greater clarity about the precise nature of the legal rights and obligations that have been created than by creating a broad civilly enforceable right to privacy.

RECOMMENDATION

22. There should be two statutory causes of action dealing with serious invasion of privacy caused by misuse of surveillance in a public place.

MISUSE OF PRIVATE INFORMATION

- 7.127 The first new cause of action should deal with serious invasion of privacy by misuse of private information. This cause of action is primarily concerned with the use of private information rather than with how it is gathered or received. It is similar in effect to the tort developed by the New Zealand courts and to the extended action for breach of confidence which is evolving in the UK courts.
- 7.128 Whether the information in question is *private* is best determined by the application of an objective test rather than by relying solely on the views of the person to whom the information relates. This approach means that the tribunal should consider values and attitudes widely held throughout the community before deciding whether the plaintiff had a reasonable expectation of privacy about the information in question. Examples of the sort of information obtained by the use of public place surveillance, which could fall within this cause of action because the plaintiff had a reasonable expectation of privacy, include footage of a person entering a medical clinic or a gay bar.

- 223 Anthony Mason, ‘Legislative and Judicial Law-Making: Can we locate an identifiable boundary?’ (2003) 24 *Adelaide Law Review* 15, 35–6.
- 224 See eg, *International Covenant of Civil and Political Rights* Art 17.
- 225 *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 13.
- 226 *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 7(1).
- 227 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199 [107] (Gummow and Hayne JJ).
- 228 Burrows, above n 218.
- 229 David Eady (Speech delivered at the University of Hertfordshire, 10 November 2009) <www.judiciary.gov.uk/docs/speeches/justice-eady-univ-of-hertfordshire-101109.pdf> at 20 April 2010.
- 230 Ibid.
- 231 (2001) 208 CLR 199 [41].
- 232 (2001) 208 CLR 199 [116].
- 233 *Wainwright v Home Office* [2004] 2 AC 406 (Lord Hoffmann).
- 234 *Hosking v Runting* [2005] 1 NZLR 1 (Gault P and Blanchard J).
- 235 Daniel Solove, *Understanding Privacy* (2008) 2.
- 236 Ibid 1.
- 237 Ibid 171.
- 238 Ibid 172.
- 239 Raymond Wacks, ‘Why there will never be an English common law privacy tort’, in Andrew T Kenyon and Megan Richardson (eds) *New Dimensions in privacy law: International and Comparative Perspectives* (2006) 183.
- 240 Ibid 177.

7.129 The gist of this cause of action is the *misuse* of private information. In most, but not necessarily all, cases the misuse of private information will involve some form of publication. This may range from photocopying documents and distributing them to others, to broadcasting footage on television or posting it on the internet. Whether the private information in question has been misused is best determined by the application of an objective test rather than by relying solely upon the views of the person to whom the information relates. Again, this approach means that the tribunal should consider values and attitudes widely held throughout the community before deciding whether the use of the private information was highly offensive. Examples of the sort of behaviour that could fall within this cause of action because the use of the private information was highly offensive to a reasonable person include publishing footage of a person entering an abortion clinic or a hospice for the dying.

RECOMMENDATION

23. The first cause of action should deal with serious invasion of privacy by misuse of private information.

INTRUSION UPON SECLUSION

7.130 The second cause of action should deal with what is often referred to as intrusion upon seclusion or spatial privacy. This cause of action is primarily concerned with the use of a surveillance device, often surreptitiously, to view parts of a person not open to public gaze or to monitor conduct that a person believes to be private. Although this cause of action has not yet been developed by the courts in New Zealand and the UK, it may emerge in time because there can be serious invasions of privacy without any publication of personal information.

7.131 The act of intruding upon a person's seclusion or invading their private space is in itself objectionable conduct. Whether a person had an entitlement to seclusion is best determined by the application of an objective test rather than by relying solely on the views of the person to whom the information relates. This approach means that the tribunal should consider values and attitudes widely held throughout the community before deciding whether the plaintiff had a reasonable expectation of privacy. Examples of the sort of things about which a person could have reasonable expectations of privacy are intimate parts of their body that are clothed and conversations that appear to be taking place well out of the earshot of others.

7.132 The gist of this cause of action is the *intrusion* upon a person's seclusion or private space. Whether the intrusion is unacceptable is best determined by the application of an objective test rather than by relying solely upon the views of the person seeking seclusion. Again, this approach means that the tribunal should consider values and attitudes widely held throughout the community before deciding whether the conduct was highly offensive. Examples of the sort of behaviour that could fall within this cause of action because the intrusion upon seclusion was highly offensive to a reasonable person include engaging in 'upskirting' on public transport or covertly listening to a conversation between people sitting on an isolated park bench.

7.133 Both examples in the previous paragraph involve criminal conduct.²⁴¹ Although the wrongdoer may be prosecuted for a criminal offence, there is no civil cause of action open to a person harmed by conduct of this nature. An action for breach of statutory duty is not available in these cases because of the limited reach of that cause of action.²⁴²

RECOMMENDATION

24. The second cause of action should deal with serious invasion of privacy by intrusion upon seclusion.

STATUTORY CAUSES OF ACTION

- 7.134 The commission believes that any new causes of action should be statutory causes of action rather than torts. As the NSWLRC pointed out, there is little to be gained—and many complex rules of law to be navigated—if any new cause of action is characterised as a tort.²⁴³ Integration within the law of torts would involve classification of the cause of action as one that is either actionable without proof of damage or that requires proof of damage.²⁴⁴ It would also involve incorporation of the detailed rules that have arisen in tort law concerning remedies and the various types of liability that may attach to actual wrongdoers and to those persons who are legally liable for the actions of others.²⁴⁵
- 7.135 Chief Justice Spigelman of the NSW Supreme Court has suggested that ‘torts’ refer to rights or causes of action generally enforceable in courts. As the commission recommends that jurisdiction in these new causes of action be vested solely in a tribunal, this observation about the ‘usual’ venue for torts is another reason why it is preferable to characterise them as statutory causes of action rather than torts.²⁴⁶

ELEMENTS

- 7.136 A number of submissions and consultations supported the creation of a cause of action for serious invasions of privacy but criticised aspects of the model proposed by the ALRC.

Should the conduct be ‘highly offensive’?

- 7.137 An important issue common to both proposed causes of action is the seriousness of the invasion of privacy. The ALRC and the NSWLRC differed on this point. The second element of the ALRC cause of action is that ‘the act or conduct complained of is highly offensive to a reasonable person of ordinary sensibilities’. The NSWLRC disagreed with this approach because, in its view, this element set the bar too high. It concluded that this element unnecessarily favoured other interests, most notably, freedom of expression, over privacy.
- 7.138 The ALRC recommended that the conduct in question be objectively highly offensive because this would help limit the cause of action to ‘egregious circumstances’²⁴⁷ and ensure that the important countervailing interest of ‘freedom of expression is respected and not unduly curtailed in the great run of circumstances’.²⁴⁸ The ALRC suggested that the requirement 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’.²⁴⁹
- 7.139 A number of individuals and organisations suggested that the requirement in the ALRC cause of action that the conduct complained of be ‘highly offensive to a reasonable person of ordinary sensibilities’ set the bar too high for the plaintiff.
- 7.140 The Law Institute of Victoria (LIV), for example, submitted that the requirement ‘could be too restrictive and too subjective to lead to consistent outcomes’.²⁵⁰ It suggested that this second element be amended to require that ‘the act complained of [be] unreasonable’, with additional guidance concerning the factors that should be taken into account in determining what is ‘unreasonable’. The LIV argued that this would be consistent with interpretations of reasonableness under the United Nations Human Rights Committee and the Victorian Charter.²⁵¹

- 241 The offence of ‘upskirting’ is dealt with in sections 41A and 41B of the *Summary Offences Act 1966* (Vic), while using a listening device to monitor a private conversation is an offence under section 6 of the *Surveillance Devices Act 1999* (Vic).
- 242 Mendelson, *The New Law of Torts*, above n 11. See esp Ch 19 for a discussion of the law of breach of statutory duty.
- 243 NSW Law Reform Commission, above n 6 [1.5].
- 244 See Mendelson, *The New Law of Torts*, above n 11. See esp Ch 1 for a discussion of classification in the law of torts.
- 245 Ibid esp Ch 21 for a discussion of remedies and Ch 22 for a discussion of the different types of liability in the law of torts.
- 246 *Commissioner of Police v Estate of Russell* (2002) 55 NSWLR 232 [70]–[75].
- 247 Australian Law Reform Commission, above n 2, 127.
- 248 Ibid [74.135].
- 249 Ibid [74.135].
- 250 Submission 27.
- 251 Submission 27.

- 7.141 According to the LIV, the application of the concept of reasonableness together with the public interest test 'would provide appropriate limits on the cause of action, such as the right to freedom of expression'.²⁵²
- 7.142 The commission believes that as legal protections for privacy develop, we should ensure that minor or trivial invasions do not divert attention away from the more significant cases. This is best done by including an element that a reasonable person of ordinary sensibilities must find the defendant's conduct to be highly offensive. In other new areas of law, such as racial and religious vilification, there are intensifiers in the statutory language used to describe unlawful conduct. Sections 7 and 8 of the *Racial and Religious Tolerance Act 2001* (Vic) prohibit conduct that incites serious contempt for, or severe ridicule of, people on racial and religious grounds. Presumably, this language has been used with the aim of ensuring that important new social policies are not undermined by adverse community responses to inconsequential claims.
- 7.143 The commission believes that the elements of the cause of action for serious invasion of privacy caused by misuse of private information should be:
- D (the defendant) misused, by publication or otherwise, information about P (the plaintiff) in respect of which he/she had a reasonable expectation of privacy; and
 - a reasonable person would consider D's misuse of that information highly offensive.
- 7.144 Similarly, the commission believes the elements of the cause of action for serious invasion of privacy caused by intrusion upon seclusion should be:
- D intruded upon the seclusion of P when he/she had a reasonable expectation of privacy; and
 - a reasonable person would consider D's intrusion upon P's seclusion highly offensive.

Intentional, reckless and negligent acts

- 7.145 The ALRC's recommended cause of action requires conduct that is deliberate or reckless, and not simply negligent. The inclusion of an element of wilfulness is consistent with the Canadian statutory privacy torts.²⁵³
- 7.146 The ALRC approach of excluding negligent acts was supported in one submission. The author of this submission supported the cause of action only if it was limited to deliberate and reckless conduct and did not extend to negligence.²⁵⁴
- 7.147 The LIV noted one possible concern with the ALRC 'state of mind' requirement. It queried whether there must be an intent to act, or an intent to invade privacy. The LIV submitted that it appears the ALRC contemplated an intent to invade privacy.
- 7.148 The commission is of the view that it is unnecessary to expressly exclude negligent acts from the conduct which might fall within the two statutory causes of action. Although it is highly likely that most serious invasions of privacy will involve intentional conduct, there may be circumstances in which a person's actions were so grossly negligent that civil action ought to be possible. An example might be a medical practitioner who leaves a patient's highly sensitive medical records on a train or tram.

RECOMMENDATIONS

25. The elements of the cause of action for serious invasion of privacy caused by misuse of private information should be:
 - a. D misused, by publication or otherwise, information about P in respect of which he/she had a reasonable expectation of privacy; and
 - b. a reasonable person would consider D's misuse of that information highly offensive.
26. The elements of the cause of action for serious invasion of privacy caused by intrusion upon seclusion should be:
 - a. D intruded upon the seclusion of P when he/she had a reasonable expectation of privacy; and
 - b. a reasonable person would consider D's intrusion upon P's seclusion highly offensive.

DEFENCES

7.149 Our Consultation Paper proposal for a statutory cause of action for serious invasions of privacy listed the three defences recommended by the ALRC,²⁵⁵ namely:

- 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.²⁵⁶

7.150 Having considered the law in other jurisdictions and the recommendations made by other law reform commissions, we believe that additional defences are desirable. They are:

- consent
- where the defendant was a public officer engaged in his or her duty and acted in a way that was not disproportionate to the matter being investigated and not committed in the course of a trespass
- where D's conduct was in the public interest, or if involving a publication, the publication was privileged or fair comment.

Consent

7.151 In the US and the UK, consent is one of the most commonly used defences in privacy actions.²⁵⁷ Consent is also an important defence in the Canadian Privacy Acts.

7.152 The ALRC did not include consent as a defence to its proposed cause of action because it believed it was unnecessary to do so. It reasoned that if a 'claimant had consented to the invasion of his or her privacy ... it is unlikely that the elements of the cause of action would be satisfied' as there would be no reasonable expectation of privacy and the conduct of the defendant would not be highly offensive.²⁵⁸

7.153 The NSWLRC included lack of consent as an element of its proposed cause of action.²⁵⁹ This means that the plaintiff would bear the burden of proof in relation to the issue of consent.

252 Submission 27.

253 *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).

254 Submission 38.

255 Victorian Law Reform Commission, *Surveillance in Public Places: Consultation Paper* Consultation Paper 7 (2009) [6.168].

256 Australian Law Reform Commission, above n 2 [74.169]. As noted above, 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.

257 Keeton, above n 126, 867-8, stating 'It has been said that chief among the defences at common law is the plaintiff's consent to the invasion' and that '[o]ther defences have appeared only infrequently' in the surveyed case law; also Helen Fenwick and Gavin Phillipson, *Media Freedom Under the Human Rights Act* (2006) 772 stating that in the UK, the most often invoked are implied consent (or 'waiver') and press freedom (or freedom of expression).

258 Australian Law Reform Commission, above n 2 [74.174].

259 NSW Law Reform Commission, above n 185 [5.46]; see also clause 74(4) of the Commission's draft bill.

7.154 The commission is of the view that consent should be an express defence to both proposed causes of action. The defendant, rather than the plaintiff, should carry the burden of proving that his or her conduct was justified by the plaintiff's consent. To do otherwise is to force the plaintiff to engage in the difficult task of proving a negative.

Protection of person or property

7.155 The defence that a person's conduct was incidental to a lawful right of defence of person or property appears in the Canadian Privacy Acts²⁶⁰ and in the recommendations of the NSWLRC and the ALRC.²⁶¹

7.156 Examples of this defence from the Canadian Acts include an employer taking privacy invasive action to prevent employee pilferage of stock,²⁶² and a defendant arguing (unsuccessfully) that his interception of his neighbour's cordless telephone conversations was protection of person since the neighbour had repeatedly threatened him.²⁶³ The defence also encompasses conduct undertaken for the purpose of prosecuting or defending civil or criminal proceedings,²⁶⁴ such as private investigations.²⁶⁵

7.157 The commission's view is that if a person's conduct was incidental to a defence of person or property it should be a defence to the proposed causes of action if the conduct is a reasonable and proportionate response to the threatened harm.

Authorised or required by law

7.158 The defence that a person's action was authorised or required by law also appears in the Canadian Privacy Acts²⁶⁶ and in the recommendations of the NSWLRC and the ALRC.²⁶⁷ This defence is important for government actors, particularly in the areas of law enforcement and national security,²⁶⁸ as it acknowledges that other laws, such as the SDA, permit them to engage in some invasions of privacy when their actions are appropriately authorised.

7.159 The commission is of the view that it should be a defence to the recommended causes of action that the defendant's conduct was authorised or required by law.

Public officer engaged in duty

7.160 The defence of being a police or public officer engaged in duties appears in the Canadian Privacy Acts. The officer must also be acting in a manner not disproportionate to the matter being investigated, and not committing a trespass.²⁶⁹

7.161 Although the defence of a police or public officer engaged in his or her duties may fall within a broad public interest defence, the commission believes it is important to provide police and public officers with a specific exception when engaged in their duties. This defence does not give police and public officers a licence to invade people's privacy. As in Canada, the conduct should be reasonable, proportionate to the duties of the officer and not involve a trespass in order to fall within the defence.

Privilege, fair comment (honest opinion) and public interest

7.162 The defences of privilege and fair comment derived from defamation law are also commonly available in privacy causes of action in other jurisdictions. So too is the defence of public interest.²⁷⁰

7.163 Although defamation is concerned with the protection of reputation, rather than privacy, the motivation for plaintiffs in a defamation action is often the desire to protect privacy or to gain compensation for an invasion of privacy.²⁷¹ In Victoria, the *Defamation Act 2005* (Vic) has replaced aspects of the common law tort of defamation.²⁷²

7.164 As the defences in defamation law seek to strike a balance between protection of a plaintiff's reputation and freedom of speech, they may also be usefully employed when seeking to strike a balance between privacy and freedom of speech.

Privilege

7.165 A privilege can be absolute or it can be qualified. Examples of absolute privilege include statements made by a member of parliament and by participants in court proceedings.²⁷³ By contrast, a qualified privilege requires the defendant to show that he or she had a legitimate duty and interest to publicise the private matter.²⁷⁴ The law protects such revelations because they promote the welfare of society.²⁷⁵ Sections 27 and 30 of the *Defamation Act 2005* (Vic) provide for a defence of absolute and qualified privilege, respectively, in any cause of action for defamation in Victoria.

7.166 Privilege is a defence in the Canadian Privacy Acts,²⁷⁶ and the NSWLRC²⁷⁷ and ALRC proposed causes of action.²⁷⁸ It is a defence to the Law Reform Commission of Ireland's proposed tort of disclosure of information obtained by privacy invasive surveillance. A 'defence'²⁷⁹ similar to the defence of qualified privilege in defamation law²⁸⁰ may be available in the UK cause of action for misuse of private information. Finally, the New Zealand Law Commission has suggested that actions that are privileged should be a defence to the New Zealand tort if they do not fall within the broad defence of legitimate public concern recognised in *Hosking v Runting*.²⁸¹

Fair comment (honest opinion)

7.167 In the interests of protecting the freedom to discuss matters of public concern, the common law developed the defence of fair comment in actions for defamation.²⁸² The fair comment defence applies when there is

1. comment based on fact
2. about a matter of public interest
3. recognisable as comment (versus fact)
4. 'fair' in the sense that 'an honest person could express the opinion, even if it is exaggerated, prejudiced or obstinate'.²⁸³

The defence may be defeated, however, by proof of malice.²⁸⁴

- 260 *Privacy Act*, RSBC 1996, c 373, s 2(2)(b); *Privacy Act*, RSM 1987, c P125, s 5(c); *Privacy Act*, RSS 1978, c P-24, s 4(1)(b); *Privacy Act*, RSNL 1990, c P-22, s 5(1)(b).
- 261 Australian Law Reform Commission, above n 2, rec 74-4(a); NSW Law Reform Commission, above n 185 [6.2].
- 262 McNairn, above n 158, 84-5 citing *United Food and Commercial Workers, Local 1400 v Saskatoon Co-operative Assn Ltd* (1992) 101 Sask R 1 (QB).
- 263 British Columbia Law Institute, above n 164, 14.
- 264 NSW Law Reform Commission, above n 185, 86.
- 265 McNairn, above n 158, 84-5 citing *United Food and Commercial Workers, Local 1400 v Saskatoon Co-operative Assn Ltd* (1992) 101 Sask R 1 (QB) and *Druken v RG Fewer and Associates Inc* (1998) 171 Nfld & PEIR 312 (Nfld TD). See also Ireland Law Reform Commission, *Privacy: Surveillance and the Interception of Communications* Report 57 (1998) 132 where, under the defence of 'fulfilling a legal duty, or exercising a legal power, or defending or maintaining a legal right', the Law Reform Commission of Ireland includes as an example where one employs a private detective to investigate another for the purpose of defending or maintaining a civil action.
- 266 *Privacy Act*, RSBC 1996, c 373, s 2(2)(c); *Privacy Act*, RSM 1987, c P125, s 5(d); *Privacy Act*, RSS 1978, c P-24, s 4(c); *Privacy Act*, RSNL 1990, c P-22, s 5(1)(c).
- 267 Australian Law Reform Commission, above n 2, rec 74-4(b); NSW Law Reform Commission, above n 185 [6.2].
- 268 As noted by Australian Law Reform Commission, above n 2 [74.171] and NSW Law Reform Commission, above n 185 [6.3].
- 269 *Privacy Act*, RSBC 1996, c 373, s 2(2)(d); *Privacy Act*, RSM 1987, c P125, s 5(e); *Privacy Act*, RSS 1978, c P-24, s 4(1)(d); *Privacy Act*, RSNL 1990, c P-22, s 5(1)(d).
- 270 Not a defence in defamation cases under the common law where truth alone is a defence. Patrick George, *Defamation Law in Australia* (2006) 243.
- 271 Mendelson, *The New Law of Torts*, above n 11, 579.
- 272 *Defamation Act 2005* (Vic) ss 6(1)-(2).
- 273 George, above n 270, (2006) 260.
- 274 *Ibid* 269.
- 275 *Ibid* quoting from the High Court in *Roberts v Bass* (2002) CLR 1, 26.
- 276 *Privacy Act*, RSBC 1996, c 373, s 2(3)(b); *Privacy Act*, RSM 1987, c P125, s 5(f)(iii); *Privacy Act*, RSS 1978, c P-24, s 4(2)(b); *Privacy Act*, RSNL 1990, c P-22, s 5(2)(b).
- 277 NSW Law Reform Commission, above n 185, [6.2].
- 278 Australian Law Reform Commission, above n 2, rec 74-4.
- 279 Lord Nicholls suggested that this issue may fall within one of the elements of the cause of action because it may affect the reasonableness of the claimant's expectation of privacy (*Campbell v MGN* [2004] 2 AC 457 [24]).
- 280 See George, above n 270, Ch 22.
- 281 *Ibid*.
- 282 *Ibid* 338.
- 283 *Ibid* 338-9.
- 284 *Ibid* 339.

7.168 The *Defamation Act 2005* (Vic) provides for a defence of honest opinion, which, though largely intended to reflect the common law, differs in some respects from the defence of fair comment.²⁸⁵

7.169 Fair comment is a defence in the Canadian Privacy Acts²⁸⁶ and the NSWLRC proposal.²⁸⁷ By contrast, the ALRC proposal does not include fair comment as a separate defence, as it is subsumed within the public interest test that is an element of the proposed cause of action.²⁸⁸

Public interest

7.170 In contrast to privilege and fair comment, where the primary concern is protection of communications, the defence of public interest may involve other matters of community concern that might justify an intrusion into privacy. The Law Reform Commission of Ireland lists the following four specific, but non-exhaustive, strands in their public interest defence:

- the detection and prevention of crime
- the exposure of illegality or serious wrongdoing
- informing the public on a matter of public importance
- preventing the public from being misled by the public utterances of public figures (broadly defined) where private beliefs and behaviour are directly at variance with the same.²⁸⁹

7.171 Freedom of expression remains a central reason for any public interest defence.²⁹⁰ For example, the New Zealand tort of invasion of privacy by publication of private facts includes the defence that the publication concerned a matter of legitimate public concern.²⁹¹

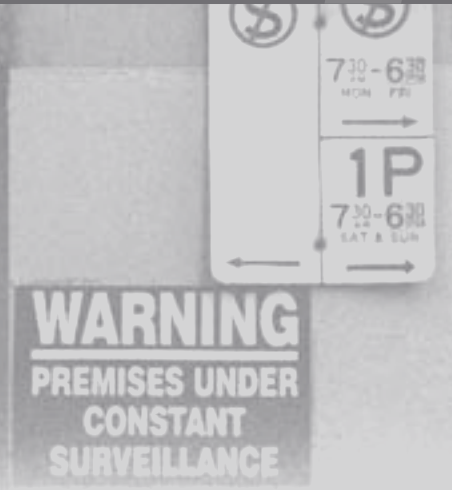
7.172 The public interest defence appears in other existing and proposed statutory causes of action for invasion of privacy. In the case of the Canadian Privacy Acts,²⁹² and the proposal of the Law Reform Commission of Ireland, the defence is limited to where there has been a publication, and so may not apply where there is surveillance without publication of the material. By contrast, in the proposals of the NSWLRC and the ALRC, where the cause of action is not limited to publication of private matters, the defence would likely apply to mere surveillance activities.²⁹³

7.173 The commission is of the view that, when devising new causes of action concerning invasion of privacy, it is important to protect revelations that would fall within the defences of privilege and honest opinion (fair comment) in defamation law. If some statements merit protection because of their value to the community, even when they are defamatory, it is strongly arguable that they should be similarly protected, even when they are invasive of privacy. Because the defences of privilege and fair comment are concerned with the publication of information, they would apply only to the proposed cause of action concerned with misuse of private information.

7.174 The public interest in protecting revelations of particular forms of conduct, such as abuse of the powers associated with public office, is widely acknowledged, even when it involves some invasion of privacy. The public interest defence should apply to both recommended causes of action. It is not logical to limit this defence to those cases that involve publication of private information because otherwise people would be encouraged to publish everything they discover that may be invasive of privacy in order to avail themselves of the defence. There will be occasions in which it ought to be possible for investigative journalists, and others, to rely upon a defence of public interest when their conduct would otherwise be an intrusion upon a person's seclusion.

- 7.175 There are different approaches to the question of which party should bear the burden of proof when the public interest is a relevant issue in a privacy dispute.
- 7.176 In an action under the New Zealand tort, the defendant bears the onus of establishing there is a legitimate public concern in the publication of otherwise private facts.²⁹⁴ The defendant also bears the onus of proof of public interest under the Canadian Privacy Acts and the Law Reform Commission of Ireland proposal.
- 7.177 In the US the plaintiff bears the burden of proof in actions for the tort of publicity given to private life. A plaintiff must show that the matter publicised is highly offensive to a reasonable person, and that it is not of legitimate concern to the public.²⁹⁵ Although the public interest is not a defence to the UK cause of action for misuse of private information, the second element of the action requires a court to balance the right to press freedom and the right to privacy.²⁹⁶
- 7.178 As both the ALRC and NSWLRC proposals treat the public interest as an element of their causes of action—the plaintiff bears the burden of proof in relation to this matter. For example, under the NSWLRC proposed cause of action, a court is required to consider ‘any relevant public interest (including the interest of the public in being informed about matters of public concern)’ when deciding whether an individual’s privacy has been invaded.²⁹⁷ In the case of the ALRC proposal, a court must take into account ‘whether the public interest in maintaining the claimant’s privacy outweighs other matters of public interest (including the interest of the public to be informed about matters of public concern and the public interest in allowing freedom of expression)’.²⁹⁸
- 7.179 The submission from legal academic David Lindsay expressed concern that requiring the plaintiff to establish that there is no countervailing public interest (such as freedom of expression) may be too high a burden because it requires the plaintiff to prove a negative.²⁹⁹
- 7.180 The commission believes that a plaintiff should not have to prove a negative, such as the lack of a countervailing public interest. The defendant should carry the burden of proof in relation to the public interest defence. The defendant should be required to introduce evidence (if necessary) and satisfy the tribunal that it was in the public interest to engage in conduct that would otherwise be unlawful.
- 7.181 In Canada and New Zealand the defendant has the burden of proof in relation to the public interest. In other areas of law involving statutory causes of action the defendant carries the burden of proof with respect to public interest considerations. Vilification law is an example in point. Under section 11 of the *Racial and Religious Tolerance Act 2001* (Vic) the defendant must establish that conduct which would otherwise be racial or religious vilification was justified because it was in the public interest. In the law of defamation, public interest considerations are dealt with as a defence rather than as one of the elements of the cause of action that must be negated by the plaintiff.³⁰⁰
- 7.182 The defence that publicity given to a private matter is justified because it concerns a matter of public interest begs the question: What is a matter of public interest? There is no settled and clear definition of public interest.³⁰¹ Rather, more commonly, there are categories believed to cover what may fall within public interest,³⁰² including:
- information needed by the public to evaluate a government official’s fitness for office
 - information for the exposure of crime, corruption and other wrongdoing in public life
 - other information affecting the public at large.³⁰³

- 285 Mendelson, above n 11, 616, 622–3.
- 286 *Privacy Act*, RSBC 1996, c 373, s 2(3)(a); *Privacy Act*, RSM 1987, c P125, s 5(f)(iii); *Privacy Act*, RSS 1978, c P-24, s 4(2)(a); *Privacy Act*, RSNL 1990, c P-22, s 5(2)(a).
- 287 NSW Law Reform Commission, above n 185, [6.2].
- 288 Australian Law Reform Commission, above n 2, [74.170].
- 289 Law Reform Commission [Ireland], above n 265, 36; Australian Law Reform Commission, above n 2 [8.10]; NSW Law Reform Commission, above n 185, [6.2].
- 290 Australian Law Reform Commission, above n 2 [74.147].
- 291 *Hosking v Runting* [2005] 1 NZLR 1[129]–[130] (Gault P and Blanchard J).
- 292 *Privacy Act*, RSBC 1996, c 373, s 2(3)(a); *Privacy Act*, RSM 1987, c P125, s 5(f)(i); *Privacy Act*, RSS 1978, c P-24, s 4(2)(a); *Privacy Act*, RSNL 1990, c P-22, s 5(2)(a).
- 293 Australian Law Reform Commission, above n 2 [74.170], where it is an element rather than a defence.
- 294 New Zealand Law Commission, above n 6, [6.63].
- 295 Restatement (Second) of Torts § 652D (1977).
- 296 Helen Fenwick and Gavin Phillipson, *Media Freedom Under the Human Rights Act* (2006) 771.
- 297 *Ibid* 86, citing NSWLRC Draft Civil Liability Amendment (Privacy) Bill 2009 s 74(2).
- 298 Australian Law Reform Commission, above n 2, rec 74–2.
- 299 Consultation 5.
- 300 George, above n 270, 338–9.
- 301 David Morrison and Michael Svennevig, ‘The Defence of Public Interest and the Intrusion of Privacy’ (2007) 8 (1) *Journalism* 44, 55.
- 302 *Ibid* 45.
- 303 Jennifer Mullaly, ‘Privacy: Are the Media a Special Case?’ (1997) 16 (1) *Communication Law Bulletin* 10, 11.



- 7.183 There are different perspectives about whether publication of any matter of interest to the public should constitute a defence to invasion of privacy. The approach of treating any subject matter that is of interest to the public as a matter of public concern is seen in the United States, where the law regards whatever the media consider to be worthy of print or broadcast as ‘newsworthy’.³⁰⁴ This approach does not distinguish between speech about celebrities’ lives and the lives of politicians, and speech about public figures and people cast into the public spotlight.³⁰⁵
- 7.184 Supporters of the approach of equating all speech with matters of public interest can point to several justifications for their stance. These include: the difficulty of distinguishing between speech of a ‘public interest’ nature and that which is not;³⁰⁶ the fact that there may never be consensus on what constitutes the public interest;³⁰⁷ the fact that information about celebrities’ lives could serve a social function, because people can model their lives on the choices celebrities make,³⁰⁸ and finally, if there is no consensus on what constitutes the public interest, who should be assigned the task of deciding what it is?³⁰⁹
- 7.185 An alternative approach avoids equating the public interest with matters that may interest the public.³¹⁰ A notable example is the 2004 decision of the European Court of Human Rights in *Von Hannover v Germany*.³¹¹ In this case, the Court concluded that Princess Caroline of Monaco’s right to private life had been breached following publication of photographs of her in public places engaged in activities such as shopping and practising sport.³¹² The Court deemed the freedom of interest values at stake to be minimal: the photos did not contribute to any debate of general interest to society, but merely satisfied the curiosity of readers about her private life.³¹³
- 7.186 Some existing and proposed causes of action for invasion of privacy attempt to exclude matters that are merely of interest to a public curious about the private lives of others from the ambit of the defence of public interest. For example, the draft legislation proposed by the Law Reform Commission of Ireland states that a disclosure ‘is not in the public interest merely because the object of such surveillance, or such information or material, is or would be newsworthy’.³¹⁴
- 7.187 The commission is of the view that not all matters of interest to the public are matters of public interest that ought to deprive a person of their right to privacy. In particular, the public interest defence ought not to extend to matters that satisfy a curiosity about the private lives of others, but serve no other purpose relevant to the common good. Tribunals and courts should be aware of this important point when interpreting and applying the proposed new laws.

Should the list of defences be exhaustive?

- 7.188 Opinions among submissions and consultations were varied on this point. The LIV queried whether having an exhaustive list of defences was advisable³¹⁵ and suggested that there might be no need to have a list of defences if the second element of the proposed cause of action for serious invasions of privacy—that the act or conduct was highly offensive to a reasonable person—is replaced with a requirement that the act or conduct was unreasonable.³¹⁶
- 7.189 The commission is of the view that the legislation should contain an exhaustive list of defences. Consent should be a defence to the proposed causes of action. The issue of the reasonableness of the defendant’s conduct is best dealt with as an element of both causes of action.

RECOMMENDATIONS

27. The defences to the cause of action for serious invasion of privacy caused by misuse of private information should be:
 - a. P consented to the use of the information
 - b. D's conduct was incidental to the exercise of a lawful right of defence of person or property, and was a reasonable and proportionate response to the threatened harm
 - c. D's conduct was authorised or required by law
 - d. D is a police or public officer who was engaged in his/her duty and the D's conduct was neither disproportionate to the matter being investigated nor committed in the course of a trespass
 - e. if D's conduct involved publication, the publication was privileged or fair comment
 - f. D's conduct was in the public interest, where public interest is a limited concept and not any matter the public may be interested in.
28. The defences to the cause of action for serious invasion of privacy caused by intrusion upon seclusion should be:
 - a. P consented to the conduct
 - b. D's conduct was incidental to the exercise of a lawful right of defence of person or property, and was a reasonable and proportionate response to the threatened harm
 - c. D's conduct was authorised or required by law
 - d. D is a police or public officer who was engaged in his/her duty and the D's conduct was neither disproportionate to the matter being investigated nor committed in the course of a trespass
 - e. D's conduct was in the public interest, where public interest is a limited concept and not any matter the public may be interested in.

EXEMPTIONS?

- 7.190 In their submissions to the commission, some organisations suggested that they, or their members, should be exempted from any new causes of action.³¹⁷ For example, Australia's Right to Know, a coalition of major media organisations, wrote:
- There is no need for any additional privacy rights or remedies in Australia. If any need for an additional privacy right or remedy is identified in future, it should be very clearly and narrowly defined and there should be a broad media exemption.*³¹⁸
- 7.191 The LIV opposed a media exemption, arguing that the balancing test in the cause of action was sufficient to protect media activities.³¹⁹
- 7.192 The Insurance Council of Australia argued that exemptions were required for the legitimate need of insurers to undertake surveillance.³²⁰ According to the Council, its 'members have a vital interest in being able to undertake surveillance in public places, for example to assess a personal injury claim (particularly for Compulsory Third Party and workers' compensation claims) and in defence of a decision to decline a claim'.³²¹

- 304 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 Restatement (Second) of Torts § 652D cmt g (1977) stating: 'To a considerable extent, in accordance with the mores of the community, the publishers and broadcasters have themselves defined the term [news]'.
- 305 Ibid 225.
- 306 Morrison, above n 301, 55.
- 307 Ibid 48.
- 308 See Richard Posner, 'The Right of Privacy' (1978) 12 *Georgia Law Review* 393, 396; Crisci, above n 304, 217.
- 309 Ibid 209.
- 310 Morrison, above n 301, 44.
- 311 *Von Hannover v Germany* 59320/00 [2004] VI Eur Court HR [61].
- 312 *Von Hannover v Germany* 59320/00 [2004] VI Eur Court HR [61].
- 313 *Von Hannover v Germany* 59320/00 [2004] VI Eur Court HR [65].
- 314 Law Reform Commission [Ireland], above n 265, 129.
- 315 Submission 27.
- 316 Submission 27.
- 317 Submissions 10, 11, 21.
- 318 Submission 28.
- 319 Submission 27.
- 320 Submission 21.
- 321 Submission 21.

- 7.193 Another group seeking an exemption was Victoria Police, who suggested police officers acting for a lawful purpose in the course of their duties should be protected from liability.³²²
- 7.194 The commission's view is that no organisations or classes of people should be exempted from the proposed statutory causes of action. The defences adequately protect people engaged in legitimate activities from unmeritorious actions for serious invasion of privacy.

REMEDIES

- 7.195 A remedy is a step or an action that a defendant is ordered to take, such as the payment of damages, once a court or tribunal finds that a wrong has been committed.

Damages

- 7.196 The most common remedy in civil actions is an order for the payment of damages. In the law of torts, damages means a court order that the defendant compensate the plaintiff monetarily for the harm caused by the defendant's wrongful conduct.³²³ Damages are usually awarded to restore a plaintiff, to the extent money can do so, to the position he or she would have been in had the wrong not been committed.³²⁴ Damages of this nature are compensatory.
- 7.197 By contrast, exemplary (or punitive) damages are designed to punish the defendant for particularly reprehensible conduct and to deter him or her (and others) from acting in this way in the future.³²⁵
- 7.198 Although exemplary damages are part of Australian law, they are rarely awarded, and only if the defendant engaged in conscious wrongdoing in flagrant disregard of the plaintiff's rights.³²⁶ Exemplary damages also raise unresolved concerns, such as whether the criminal law, with its safeguards for defendants, might be the more appropriate forum for punishing a wrongdoer and whether their award may amount to an unfair windfall for the plaintiff.³²⁷
- 7.199 Exemplary damages have been awarded at common law in defamation cases.³²⁸ However, section 37 of the *Defamation Act 2005* (Vic) now provides that exemplary damages cannot be awarded in defamation actions. As the NSW Court of Appeal recently noted:

*Parliament has tended to cut down exemplary damages at common law. Secondly, in the fields where Parliament has created new rights or developed existing rights, it has generally not conferred a right to exemplary damages.*³²⁹

- 7.200 Neither the ALRC nor the NSWLRC proposed that causes of action for invasion of privacy provide for exemplary damages.

Proof of actual damage

- 7.201 Some torts, such as assault, trespass and defamation, are actionable per se,³³⁰ meaning that the plaintiff may be awarded 'damages at large' without the need to prove any actual injury or economic loss caused by the defendant's wrongdoing.³³¹ In cases of this nature damages may be awarded to compensate the plaintiff for infringement of his or her dignity, honour or decorum.³³² The practical effect is to allow the plaintiff to be compensated for insult and humiliation,³³³ without the need to prove injury or economic loss, which is necessary when actual damage forms part of the cause of action.

7.202 In most of the jurisdictions we reviewed proof of actual damage is unnecessary in privacy actions. The Court of Appeal in *Hosking v Runting* made it clear that under the New Zealand privacy tort, proof of actual damage in the sense of ‘personal injury or economic loss’ is unnecessary and the ‘harm to be protected against is in the nature of humiliation and distress’.³³⁴ Similarly, proof of damage is unnecessary under the Canadian Privacy Acts,³³⁵ and in the proposal of the Law Reform Commission of Ireland for a tort of privacy-invasive surveillance.³³⁶ The ALRC and NSWLRC proposals for a cause of action for invasion of privacy are also actionable without proof of damage.³³⁷

Limits to the amount of damages

7.203 Caps to the amount of compensation a court may award for non-economic loss are common in Australia.³³⁸ Their purpose is to ensure that awards are not too high, given that non-economic, as opposed to economic, loss cannot be precisely quantified. Under the *Defamation Act 2005* (Cth), for example, the maximum amount of damages that a court may award in defamation cases is generally \$250 000.³³⁹

7.204 Damages awards in invasion of privacy and breach of confidence cases in Australia and elsewhere have not been excessive. In *Giller v Procopets*,³⁴⁰ the plaintiff was awarded \$50 000 damages (including aggravated damages) for non-economic loss; in *Jane Doe v ABC*³⁴¹ the plaintiff was awarded \$110 000 for non-economic loss; and in *Grosse v Purvis*,³⁴² the plaintiff was awarded \$108 000 for non-economic loss.

7.205 Damages awards have ranged from small to moderate in both Canada and the UK. In the UK, Mosley attracted the largest award, £60 000.³⁴³

7.206 The NSWLRC proposal places a cap on the award of damages for non-economic loss at \$150 000, adjustable yearly based on average weekly total earnings of full-time adults over the preceding four quarters. This is the form of adjustment used in the *Civil Liability Act 2002* (NSW), which deals with actions in tort.³⁴⁴

Injunctions

7.207 An injunction is a remedy that may have an important role to play in some invasion of privacy cases. We use the term ‘injunction’ broadly to mean any order of a tribunal or court that compels specified conduct. In some instances, an injunction may be sought to prevent the initial publication of material, while in others it may be sought to prevent its ongoing publication in forums such as websites. Sometimes it may be appropriate to direct a person to publish an apology in response to the wrongful publication of private information, or to apologise privately for an intrusion upon seclusion.

7.208 An injunction may be sought to stop the threatened publication of private information. This step is particularly challenging in cases involving privacy interests because of the irreparable consequences of publication. Justice Eady suggested in *Mosley* that ‘an infringement of privacy cannot ever be effectively compensated by a monetary award’,³⁴⁵ and observed that ‘once privacy has been infringed, the damage is done and the embarrassment is only augmented by pursuing a court action’.³⁴⁶

7.209 The British courts have issued injunctions to prevent the initial publication, or continued publication, of material in some misuse of private information cases. Injunctions have prevented publication of the addresses of convicted murderers when released from prison,³⁴⁷ the details of the extra-marital sex life of a football player,³⁴⁸ the private life of a musician,³⁴⁹ and the musings of Prince Charles in his diary.³⁵⁰

322 Submission 11.
 323 See eg, Mendelson, above n 10, 31.
 324 George, above n 278, 370.
 325 NSW Law Reform Commission, *Invasion of Privacy*, Consultation Paper, above n 5 [8.11].
 326 *Gray v Motor Accident Commission* (1998) 196 CLR 1, 5, 9.
 327 See Ibid 42–3 discussing *Gray v Motor Accident Commission* (1998) 196 CLR 1 and Rachael Mulheron, ‘Exemplary Damages and Tort: an International Comparison (2000) 2 UNDALR 17. But see *Gray v Motor Accident Commission* (1998) 196 CLR 1, 7 (Gleeson CJ, McHugh, Gummow and Hayne JJ) noting that there is tension between using civil proceedings to compensate a party who is wronged and using the same proceedings to punish the wrongdoer only if it is assumed there is a sharp dividing line between the criminal law and the law of torts and contract, and noting the intermingling of criminal and civil law, such as ‘the increasing frequency with which civil penalty provisions are enacted’.
 328 *Uren v John Fairfax & Sons Pty Ltd* (1966) 117 CLR 118.
 329 *Harris v Digital Pulse Pty Ltd* [2003] NSWCA 10 at [296].
 330 Meaning literally, ‘by itself’.
 331 Mendelson, above n 10, 46.
 332 Ibid 46.
 333 Australian Law Reform Commission, above n 2 [74.167] citing Francis Trindade, Peter Cane, Mark Lunney, *The Law of Torts in Australia* (3rd ed, 1999) 23.
 334 *Hosking v Runting* [2005] 1 NZLR 1[128] (Gault P and Blanchard J).
 335 *Privacy Act*, RSS 1978, c P–24, s 2; *Privacy Act*, RSBC 1996, c 373, s 1(1); *Privacy Act*, RSM 1987, c P125, s 2(2); *Privacy Act*, RSNL 1990, c P–22, s 3(1).
 336 Law Reform Commission [Ireland], above n 265 [7.28].
 337 Australian Law Reform Commission, above n 2 rec 74–3(b); NSW Law Reform Commission, *Invasion of Privacy*, Report, above n 185 [7.9].
 338 NSW Law Reform Commission, above n 185 (2009) [7.11] citing Harold Luntz, *Assessment of Damages for Personal Injury and Death* (4th ed) (2002) [11.2.1]–[11.2.22].
 339 *Defamation Act 2005* (Cth) s 35(1).
 340 [2008] VSCA 236 [443]–[446].
 341 [2007] VCC 281.
 342 [2003] QDC 151.
 343 *Mosley v News Group Newspapers Limited* [2008] EWHC 177 (QB) [231].
 344 NSW Law Reform Commission, *Invasion of Privacy*, Report, above n 185 [7.13].
 345 *Mosley v News Group Newspapers Limited* [2008] EWHC 177 (QB) [231].
 346 *Mosley v News Group Newspapers Limited* [2008] EWHC 177 (QB) [230].
 347 *Venables v News Group Newspapers Ltd* [2001] Fam 430.
 348 *A v B plc* [2003] QB 195.
 349 *McKennitt v Ash* [2008] QB 73.
 350 *Associated Newspapers Ltd v HRH Prince of Wales* [2008] Ch 105.

- 7.210 Importantly, there have also been high profile cases in which the courts have declined to restrain publication of material that may be invasive of privacy. In *John Terry v Persons Unknown*,³⁵¹ Tugendhat J rejected an application for an injunction against the media to prevent publication of information about an affair involving the captain of the English football team. The judge was not satisfied that the plaintiff was likely to succeed in defeating a defence that it would be in the public interest for there to be publication.³⁵²
- 7.211 A number of law reform bodies have discussed the importance of injunctions as a remedy for privacy invasion cases. For example, because the British Columbia Privacy Act, unlike the other three Canadian Privacy Acts, does not deal with remedies expressly, the British Columbia Law Institute recently recommended that the Act be amended to confer power on the courts to grant remedies other than damages. In particular, the Institute noted the importance of injunctions ‘to make civil privacy legislation useful in curbing a privacy violation of a persistent nature’.³⁵³
- 7.212 Similarly, the Law Reform Commission of Ireland recommended an injunction, or ‘privacy order’, be a remedy for its proposed torts. The Commission has written that injunctions are ‘a key feature in any strategy to enhance the protection of privacy, as privacy is a highly perishable commodity’.³⁵⁴
- 7.213 Because injunctions impede media freedom, the common law has generally disfavoured ‘prior restraint’ on publication.³⁵⁵ In the US, injunctions may not be readily awarded in privacy invasion cases.³⁵⁶ In *Hosking v Runting* members of the New Zealand Court of Appeal referred to the legitimate concerns of the media with respect to injunctions and ‘prior restraint’.³⁵⁷ The justices in the majority suggest that an injunction should not be granted to restrain publication unless there is ‘compelling evidence of most highly offensive intended publicising of private information and there is little legitimate public concern in the information’.³⁵⁸

Declarations

- 7.214 A declaration is an order of a court or tribunal that contains a statement about the legal rights and obligations of a party to a dispute. In some cases involving misuse of private information or intrusion upon seclusion, the plaintiff may seek little more than a public finding, by way of declaration, that he or she has been wronged. For example, a court or tribunal could declare that the publication in a newspaper of the naked image of an identifiable person, originally obtained by the use of a wave scanner, was a wrongful use of private information. In some instances a declaration of this nature may be sufficient solace for the wronged person.
- 7.215 We received only one submission about the remedies that should be available when there has been a serious invasion of privacy.
- 7.216 The LIV suggested there may be circumstances in which exemplary damages would be appropriate.³⁵⁹ Specifically, the LIV would ‘prefer to leave it to the adjudicator’s discretion as to whether exemplary damages should be awarded’.³⁶⁰
- 7.217 The commission is of the view the remedies for the two proposed causes of action should be
- compensatory damages
 - injunctions
 - declarations.

7.218 We do not include exemplary damages. It is our view that the available damages should be compensatory only. Criminal proceedings and civil penalty proceedings should be the sole means of punitive action against any person for grossly offensive behaviour falling within either of the proposed statutory causes of action.

7.219 Further, in view of the modest sums likely to be awarded in cases of this nature, the commission believes that a statutory cap on damages is unnecessary. It should be possible for the plaintiff to be compensated for insult and humiliation without the need to prove injury or economic loss.

COSTS

7.220 The question of who should be responsible for paying the costs of any civil legal proceedings is often complicated. The usual costs rule in the courts—that the losing party should be required to pay the costs of the winning party—can be a strong disincentive to the vindication of legal rights when the sum of money that may be awarded in damages to a successful plaintiff is small. A simple risk:benefit analysis will often lead to the conclusion that it is not worth the risk of litigating, especially when an adverse legal costs order may be much greater than any award of damages. Only the wealthy can afford the risk in these circumstances.

7.221 Two leading English cases illustrate this point. Supermodel Naomi Campbell risked over £1 million in costs for a damages award of £3500,³⁶¹ while motor racing impresario Max Mosley succeeded in gaining £60 000 in damages and £850 000 in legal costs.³⁶² Litigation of this nature is beyond the reach of ordinary members of the community.

7.222 The fairest way to deal with costs in cases of this nature is to start from the position that each party should be responsible for their costs but to permit departures from this presumption when it is fair to do so. This rule guards against the abuse of legal process because the decision-maker can award costs against a plaintiff who takes frivolous proceedings and against a defendant who seeks to exhaust the resources of the plaintiff by unnecessarily prolonging the case.

7.223 Costs should be dealt with in accordance with section 109 of the *Victorian Civil and Administrative Tribunal Act 1998* (Vic) (VCAT Act). That section provides that each party is to bear their own costs in the proceeding, unless the Tribunal orders one party to pay all or a part of the costs of the other party, if that would be fair to do so.³⁶³

RECOMMENDATION

29. The remedies for both causes of action should be:

- a. compensatory damages
- b. injunctions
- c. declarations.

30. Costs should be dealt with in accordance with section 109 of the VCAT Act.

JURISDICTION

7.224 It is necessary to consider which body should have jurisdiction to hear cases involving the proposed new causes of action for misuse of private information and intrusion upon seclusion.

351 [2010] EWHC 119 (QB).

352 [2010] EWHC 119 (QB) [149].

353 British Columbia Law Institute, above n 164, 41.

354 Law Reform Commission [Ireland], above n 265 [7.31].

355 NSW Law Reform Commission, above n 185 citing William Blackstone, *Commentaries on the Laws of England* (1769) vol 4, 151–2; *Australian Broadcasting Corporation v O’Neill* (2006) 227 CLR 52, [260]–[268] (Heydon J dissenting).

356 Robert Gellman, ‘A General Survey of Video Surveillance in the United States’ in Sjaak Nouwt et al (eds) *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy* (2005), 7, 34.

357 *Hosking v Runting* [2005] 1 NZLR 1[151] (Gault P and Blanchard J).

358 *Hosking v Runting* [2005] 1 NZLR 1[158] (Gault P and Blanchard J).

359 Submission 27.

360 Submission 27.

361 *Campbell v MGN Ltd* [2005] 2 AC 457.

362 ‘Mosley Wins £60,000 in Privacy Case’ *Metro*, 24 July 2008 <www.metro.co.uk/news/article.html?in_article_id=233683&in_page_id=34> at 19 November 2009.

363 S 109 (1)–(3) *Victorian Civil and Administrative Tribunal Act 1998* (Vic).

Statutory Causes of Action

7.225 A number of submissions in response to our Consultation Paper supported giving jurisdiction to VCAT rather than to the courts.³⁶⁴ Among them, the LIV argued:

*Giving powers to the Victorian Privacy Commissioner or the Victorian Civil and Administrative Tribunal to adjudicate actions for privacy invasions could make the action more accessible to people and therefore more appropriate than actions in the courts.*³⁶⁵

7.226 The commission agrees with this view. VCAT is designed to be more accessible than the courts. It seeks to be a speedy, low-cost tribunal where legal costs do not outweigh the issues at stake. The experience in other jurisdictions demonstrates that any damages awards in cases of this nature are likely to be relatively small. The sums of money involved do not justify the level of legal costs usually associated with civil litigation in the courts. The costs associated with the high profile UK cases involving Naomi Campbell and Max Mosley could be replicated in Victoria if there were to be protracted litigation in the Supreme Court.

7.227 The likely nature of cases concerning the two proposed statutory causes of action also supports the view that jurisdiction should be vested in VCAT rather than the courts. Courts are well equipped to conduct civil litigation involving complex issues of law or fact. Court rules concerning pleadings are designed to identify contested questions of law and fact so that the parties and the court can direct their attention to matters that require adjudication. Court rules concerning the admissibility and use of evidence seek to ensure that contested issues of fact are determined as fairly as possible.

7.228 Cases concerning the two proposed statutory causes of action are unlikely to involve contested and complex issues of law or fact. They may involve judgment, however, about contested issues of privacy and community standards. VCAT is well placed to undertake these tasks because of its experience in exercising jurisdiction under the *Information Privacy Act 1999* (Vic) and because of the broad range of members upon which it may draw to hear cases of this nature. There will be some opportunity for input by the courts because the Supreme Court hears appeals from VCAT on questions of law.³⁶⁶

RECOMMENDATION

31. Jurisdiction to hear and determine the causes of action for serious invasion of privacy by misuse of private information and by intrusion upon seclusion should be vested exclusively in the Victorian Civil and Administrative Tribunal.

AVAILABILITY OF THE CAUSE OF ACTION TO CORPORATIONS AND DECEASED PERSONS

7.229 It is important to consider whether corporations and deceased persons, as well as living individuals, should have the right to take action for misuse of private information or intrusion upon seclusion.

Corporations

7.230 Although the law has assigned many of the attributes of individuals to corporations,³⁶⁷ it does not make all causes of action available to corporations, and sometimes restricts the claims they can make.³⁶⁸ For example, while a corporation could sue for defamation at common law, it could not claim injury to feelings and was restricted to a claim for financial loss.³⁶⁹ Under section 9 of the *Defamation Act 2005* (Vic), corporations no longer have a cause of action for defamation, unless they are small businesses or not-for-profit organisations.³⁷⁰

- 7.231 Some members of the High Court have suggested that any common law tort of invasion of privacy should not be available to corporations. In *Lenah Game Meats*,³⁷¹ Gummow and Hayne JJ said that the plaintiff was an ‘artificial legal person [which] lacks the sensibilities, offence and injury to which provide a staple value for any developing law of privacy’.³⁷² In the same case Gleeson CJ said that because the concept of privacy involves the protection of human dignity, it ‘may be incongruous when applied to a corporation’.³⁷³
- 7.232 As the NSWLRC recently noted, jurisdictions with existing privacy causes of action typically allow only ‘natural persons’ (that is, human beings) to bring the action.³⁷⁴ For example, the Restatements of US law states that, other than in actions for appropriation of one’s name or likeness, an action for invasion of privacy can only be brought by a living individual.³⁷⁵ The Privacy Act of the Canadian province of Newfoundland and Labrador limits the cause of action to natural persons,³⁷⁶ and the British Columbia Law Institute has recently recommended that the British Columbia Act be amended to make it clear that it does not confer a right of action upon corporations for any violation of privacy.³⁷⁷
- 7.233 Other law reform commissions have favoured limiting proposed privacy rights of action to natural persons. The ALRC proposed cause of action for an invasion of privacy is not available to corporations.³⁷⁸ The ALRC has reasoned that ‘extending the protection of a human right to an entity that is not human is inconsistent with the fundamental approach of Australian privacy law’.³⁷⁹ The Law Reform Commission of Ireland has similarly observed that corporate bodies do not have personal space that can be invaded in the same way as individuals, and no human rights objectives, such as dignity or autonomy, compel the application of the protections offered by their proposed torts to corporations.³⁸⁰ The NSWLRC draft legislation for a cause of action for invasion of privacy also limits the action to humans by using the term ‘individual’ when describing the right of action.³⁸¹
- 7.234 Corporations may have some privacy-related interests. The British Columbia Law Institute has observed that ‘corporations have their secrets and may suffer economic damage from disclosure of certain kinds of information, such as the details of an unpatented process or competitively sensitive production cost data’.³⁸² However, according to the Institute, a right of action for invasion of privacy is best restricted to natural persons, because corporations have other remedies available to them, such as causes of action for breach of contract, breach of fiduciary duty, trespass, and nuisance by which they may enforce confidentiality agreements or prevent physical or electronic intrusion onto their premises.³⁸³

Deceased persons

- 7.235 Both the NSWLRC and the ALRC have recommended that any causes of action for invasion of privacy should be restricted to living persons. Clause 79 of the draft legislation proposed by the NSWLRC for a statutory cause of action for invasion of an individual’s privacy states that the action does not survive the death of the individual.³⁸⁴ The ALRC’s proposed cause of action for a serious invasion of privacy is limited to ‘natural persons’,³⁸⁵ and in the context of the *Privacy Act 1988* (Cth), the ALRC has written that the right to privacy ‘attaches to the individual and should not survive the death of the individual’.³⁸⁶
- 7.236 Deceased persons have no right of action under defamation law. At common law, a deceased person’s estate or family members have no right to sue for defamation on that person’s behalf.³⁸⁷ Section 10(a) of the *Defamation Act 2005* (Vic) prohibits a person from asserting, continuing, or enforcing a cause of action for defamation in relation to the publication of defamatory matter about a deceased person.

- 364 Submissions 27, 40.
 365 Submission 27.
 366 *Victorian Civil and Administrative Tribunal Act 1998*, s 148.
 367 Harold Ford, R Austin, Ian Ramsay, *Ford’s Principles of Corporations Law* (13th ed) (2007) [4.050].
 368 *Ibid*.
 369 *Ibid* citing *Lewis v Daily Telegraph Ltd* [1964] AC 234 at 262 per Lord Reid.
 370 See also George, above n 270, 399.
 371 *Australian Broadcasting Corporation v Lenah Game Meats Pty Limited* (2001) 208 CLR 199.
 372 *Australian Broadcasting Corporation v Lenah Game Meats Pty Limited* (2001) 208 CLR 199, 256 [126].
 373 *Australian Broadcasting Corporation v Lenah Game Meats Pty Limited* (2001) 208 CLR 199, 226 [43].
 374 NSW Law Reform Commission, above n 6, 180.
 375 Restatement (Second) of Torts § 652I (1977).
 376 By referring only to the privacy of an individual, and defines an individual to mean ‘natural person’ (ie, a human being). *Privacy Act*, RSNL 1990, c P-22, ss 2, 3(1).
 377 British Columbia Law Institute, above n 164, rec 6.
 378 Australian Law Reform Commission, above n 2 [74.160] rec 74-3(a).
 379 *Ibid* [74.160].
 380 Law Reform Commission [Ireland], above n 265 [7.33].
 381 NSW Law Reform Commission, above n 185, 85.
 382 British Columbia Law Institute, above n 164, 44.
 383 *Ibid* 45.
 384 NSW Law Reform Commission, above n 185, 71, 89.
 385 Australian Law Reform Commission, above n 2, rec 74-3(a).
 386 Australian Law Reform Commission, above n 2 [8.44].
 387 George, above n 270, 174.

- 7.237 The rationale for excluding deceased persons from a right of action for defamation or privacy is that deceased persons cannot suffer any insult to reputation or dignity and cannot incur the injury to feelings and mental distress that flows from these insults.
- 7.238 It is arguable, however, that in some instances deceased persons may have an interest in the privacy of their personal information past death. For example, under the Law Reform Commission of Ireland's proposed privacy torts, a right of action is available to representatives of deceased persons, where the remedy sought is a privacy order, rather than damages or an account of profits.³⁸⁸ The former would allow the family or estate of a deceased person to seek delivery of materials, such as private or confidential documents, from a defendant.³⁸⁹
- 7.239 Similarly, the ALRC has recommended amendments to the *Privacy Act 1988* (Cth) to protect the personal information of persons who have been dead for 30 years or less where the information is held by an organisation.³⁹⁰ According to the ALRC, the protections provided by the Privacy Act are analogous to the protections offered by legal duties of confidentiality, which do survive the death of an individual.³⁹¹ The reforms they suggest aim to ensure that 'living individuals are confident to provide personal information, including sensitive information, in the knowledge that the information will not be disclosed in inappropriate circumstances after they die'.³⁹²
- 7.240 The commission is of the view that the causes of action for misuse of private information and intrusion upon seclusion should be available to natural persons only, and not to corporations or deceased people.
- 7.241 Limiting privacy rights of action to living human beings is consistent with other jurisdictions, the views expressed by some High Court judges, defamation law, and the recommendations of other law reform commissions. This approach is also consistent with the Charter, which stipulates that human rights, such as the right to privacy,³⁹³ are applicable to human beings only.³⁹⁴
- 7.242 Although there may be some legitimate reasons for protecting the privacy of people's personal information past death, these interests are best protected by implementing the ALRC's recommendations with respect to the *Privacy Act 1988* (Cth) rather than conferring a right of action upon the estate of a deceased person.

RECOMMENDATION

32. These causes of action should be restricted to natural persons. Corporations and the estates of deceased persons should not have the capacity to take proceedings for these causes of action.

LIMITATION OF ACTION

- 7.243 A plaintiff in a defamation action has one year from the date of publication of the defamatory matter to bring the action.³⁹⁵ A court can extend this limitation period to up to three years if satisfied that it was not reasonable in the circumstances for the plaintiff to have commenced the action within one year of publication.³⁹⁶
- 7.244 The NSWLRC's proposal for a cause of action for invasion of privacy takes a similar approach. There is a limitation period of one year, running from the date of the defendant's conduct,³⁹⁷ and an extension of the limitation period to up to three years from the date of the defendant's conduct if the court is satisfied it was not reasonable in the circumstances for the plaintiff to have commenced the action within the year.³⁹⁸

7.245 According to the NSWLRC, a one-year limitation period is generally appropriate because 'if the invasion is serious enough, the plaintiff will, and should, act promptly to avoid any escalation in the impact of the injury'.³⁹⁹ Moreover, the court's ability to extend the limitations period to up to three years allows for cases where, for example, a plaintiff was not aware of the defendant's conduct during that one year period.⁴⁰⁰

7.246 However, the NSWLRC did not favour a general rule that the cause of action accrue from the time the plaintiff first became aware of the invasion of privacy. According to the NSWLRC:

*Such an approach would not cohere with the general approach to the law of limitations in Australia and would, we believe, be difficult to achieve as part of an exercise in uniformity of law in Australia.*⁴⁰¹

7.247 By contrast, the Law Reform Commission of Ireland recommended that under its proposed statutory torts, an action be barred after a period of three years commencing from the date the plaintiff became aware (or ought reasonably to have become aware) of the tort and of the identity of the defendant.⁴⁰²

7.248 The commission is of the view that a plaintiff should bring the action within three years of the date the cause of action arose, that being the date of the defendant's conduct. This step would ensure actual consistency with causes of action for personal injuries,⁴⁰³ and practical consistency with causes of action for defamation where the limitation period can be extended to up to three years if the reason for the delay in not commencing proceedings within 12 months can be reasonably explained.⁴⁰⁴

RECOMMENDATION

33. Proceedings must be commenced within three years of the date upon which the cause of action arose.

CONCLUSION

7.249 We have recommended the introduction of two statutory causes of action in response to serious invasions of privacy: the first dealing with misuse of private information, the second with intrusion upon seclusion.

7.250 Although our focus has been to establish an appropriate legal response to the misuse of surveillance in public places, these new causes of action would not be limited to surveillance practices and conduct in public places. Rather, they would apply to all instances of misuse of private information and intrusion upon seclusion.

7.251 Evidence from other jurisdictions with similar causes of action suggests that their availability is unlikely to lead to a flood of litigation and increased expense for users of public place surveillance.

388 Law Reform Commission, above n 265, 142–3.

389 Ibid 142–143.

390 Australian Law Reform Commission, above n 2, rec 8–1.

391 Australian Law Reform Commission, above n 2 [8.1]–[8.3].

392 Ibid [8.3].

393 The right to privacy is recognised in section 13 of the *Charter of Human Rights and Responsibilities Act 2006* (Vic).

394 *Charter of Human Rights and Responsibilities Act 2006* (Vic), s 6(1).

395 *Limitation of Actions Act 1958* (Vic) s 5 (1AAA).

396 *Limitation of Actions Act 1958* (Vic), s 23B.

397 NSW Law Reform Commission, above n 185 [9.1].

398 Ibid [9.1].

399 Ibid [9.2].

400 Ibid [9.2].

401 Ibid [9.2].

402 Law Reform Commission [Ireland], above n 265 [7.37].

403 *Limitation of Actions Act 1958* (Vic), s 5(1AA).

404 *Limitation of Actions Act 1958* (Vic), s 23B.

Appendices

CONTENTS

- 170 Appendix A: Submissions
- 172 Appendix B: Consultative Committee, Community Forums, Consultations and Site Visits
- 174 Appendix C: Preliminary Roundtable Consultations

Appendix A

SUBMISSIONS

SUBMISSIONS	
1	Pastor Richard D T Wilson
2	Anonymous
3	Victorian Taxi Directorate, Victorian Department of Transport
4	Lilydale Centre Safe Committee Inc
5	Liberty Victoria
6	Francis and Leonie Osowski
7	Office for Youth, Department of Planning and Community Development
8	Australian Hotels and Hospitality Association Incorporated
9	Human Rights Law Resource Centre Ltd
10	Australian Press Council
11	Victoria Police
12	Youthlaw Inc
13	Anonymous
14	St Kilda Legal Service Co-op Limited
15	Victorian Association of Photographic Societies
16	Suncorp-Metway Ltd
17	Les Simmonds and Associates Pty Ltd
18	Harm Reduction Victoria Inc
19	Sensis Pty Ltd
20	Victorian Aboriginal Legal Service Cooperative Ltd
21	Insurance Council of Australia
22	Property Council of Australia
23	Confidential
24	Investment and Financial Services Association Ltd
25	Shopping Centre Council of Australia
26	Australian Security Industry Association Limited
27	Law Institute Victoria
28	Right to Know Coalition
29	Office of the Victorian Privacy Commissioner
30	Victorian Alcohol and Drug Association
31	Confidential
32	Youth Affairs Council of Victoria Inc
33	ART Security Pty Ltd

SUBMISSIONS	
34	Fitzroy Legal Service
35	Office of the Privacy Commissioner, Australia
36	Women's Legal Service Victoria
37	Anonymous
38	Anonymous
39	Anonymous
40	Federation of Community Legal Centres Victoria
41	Biometrics Institute
42	Homeless Persons' Legal Clinic, Public Interest Law Clearing House
43	Islamic Council of Victoria
44	Confidential

Appendix B

CONSULTATIVE COMMITTEE, COMMUNITY FORUMS, CONSULTATIONS AND SITE VISITS

CONSULTATIVE COMMITTEE

Louise Connor	Secretary (Victoria), Media and Arts Alliance
Andy Frances	Manager, Security and Venue Support, Melbourne Cricket Club
Leigh Gassner	Former Assistant Commissioner, Region 1 (CBD), Victoria Police
Moira Paterson	Associate Professor, Monash University Faculty of Law
Michael Pearce SC	President, Liberty Victoria
Bill Penrose	Vice President, Victorian Local Governance Association
Jen Rose	Manager, Policy and Projects, Youth Affairs Council of Victoria
Helen Versey	Victorian Privacy Commissioner
Dr Deane Wilson	Senior Lecturer in Criminology, Monash University

COMMUNITY FORUMS

1	Neighbourhood Justice Centre
2	Centre for Multicultural Youth
3	Youthlaw Inc and Youth Affairs Council of Victoria Inc
4	Homeless Persons' Legal Clinic, Public Interest Law Clearing House
5	Ethnic Communities Council of Victoria

CONSULTATIONS

1	Shopping Centre Council of Australia and Westfield Shopping Australia
2	Transport Certification Australia Limited
3	Confidential
4	Keeper of Evidence, Department of Transport
5	Dr David Lindsay
6	Director of Liquor Licensing, Department of Justice
7	Service Station Association Ltd
8	Confidential
9	Nigel Waters
10	Melbourne City Council
11	Woolworths Limited
12	Broadcast media
13	Confidential
14	Print media
15	Office of Policy Integrity
16	Radio Frequency Identification Association of Australia
17	ART Security Pty Ltd

CONSULTATIONS

18	Australian Security Industry Association Limited
19	Victoria Police
20	Victoria Police
21	Victoria Police
22	Lilydale Centre Safe Committee Inc
23	Office of the Special Investigations Monitor
24	Confidential
25	Victoria Police
26	Confidential
27	Geelong City Council employees
28	Victorian Equal Opportunity and Human Rights Commission
29	Confidential
30	Confidential
31	Private investigators
32	Commissioner for Law Enforcement Data Security

SITE VISITS

1	VicRoads
2	Southern Cross Station
3	Federation Square
4	Connex
5	Melbourne City Council
6	Etihad Stadium
7	Connex Metro Train Control
8	Victorian Taxi Directorate
9	Citylink
10	Chasers Nightclub
11	State Library of Victoria
12	Melbourne Sports and Aquatic Centre
13	Crown Casino
14	Melbourne Cricket Ground
15	Westfield Shopping Centre, Airport West
16	Myer, Doncaster
17	L3 Communications
18	Department of Housing

Appendix C PRELIMINARY ROUNDTABLE CONSULTATIONS

ROUNDTABLES		
1	Policy I	Melbourne Magistrates Court; Director of Liquor Licensing, Department of Justice; Office of Housing Department of Housing; Privacy Victoria; Policy Division, Department of Justice
2	Policy II	Tourism Victoria; Victorian WorkCover Authority; Office for Youth, Department of Planning and Community Development; Department of Sustainability and Environment; Department of Human Services; Office of Small Business; Department of Education and Early Childhood Development; Consumer Affairs Victoria
3	Transport I	Department of Infrastructure; VicRoads; V/Line; Transport Accident Commission
4	Sports and entertainment (government)	Melbourne Exhibition Centre; Melbourne Cricket Ground Trust; National Gallery of Victoria; Museum Victoria; Victorian Arts Centre Trust; Film Victoria; Parks Victoria
5	Victoria Police	Victoria Police
6	Local government I	Municipal Association of Victoria; City of Stonnington; City of Port Phillip; City of Ballarat; City of Greater Geelong; Lilydale Safe Centre Committee
7	Local government II	City of Melbourne; Darebin City Council; City of Greater Dandenong
8	Local government and Victoria Police	Latrobe City Council; Victoria Police
9	Tertiary education	Victoria University; Ballarat University; Melbourne University; Monash University; Swinburne University of Technology; Royal Melbourne Institute of Technology; Deakin University
10	Sports, entertainment, education and transport (government)	Department of Innovation, Industry and Regional Development; Victorian Taxi and Tow Truck Directorate; Port of Melbourne Corporation; State Sport Centres Trust; Holmesglen Institute of TAFE; Box Hill Institute of TAFE; Kangan Batman Institute of TAFE.
11	Racing (government and private)	Office for Racing, Department of Justice; Greyhound Racing Victoria; Racing Victoria Limited
12	Gaming and transport (government)	Department of Justice; Department of Infrastructure; Victorian Commission for Gambling Regulation
13	Sports and entertainment (private)	Federation Square; Telstra Dome; Clubs Victoria; Crown Casino; Marriner Theatres
14	Retail I	Queen Victoria Market; Coles Group; Institute of Body Corporate Managers
15	Retail II	Pharmacy Guild of Australia; Woolworths Limited; Myer; Colonial First State Property Management; Australian Retailers Association
16	Community representatives and private citizens I	Youthlaw Inc; Human Rights Law Resource Centre; Homeless Persons' Legal Clinic, Public Interest Law Clearing House

ROUNDTABLES		
17	Community representatives and private citizens II	Youth Affairs Council of Victoria Inc; Mental Health Legal Centre; Electronic Frontiers; Liberty Victoria
18	Community representatives and private citizens III	Welfare Rights Unit; Victorian Council of Social Services; Islamic Council of Victoria; Australian Privacy Foundation
19	Transport II	CityLink; Southern Cross Station; Bus Association of Victoria; National Intelligent Transport Systems Centre; Yarra Trams
20	Transport, retail and services (private)	Shopping Centre Council of Australia; Victorian Automobile Chamber of Commerce; Victorian Authorised Newsagents Association; Fitness Victoria; RACV
21	Utilities and services (government)	Neighbourhood Watch Victoria; Crime Stoppers Victoria; Yarra Valley Water; South East Water
22	Young people	Youth Affairs Council of Victoria (Members); Youth Workers; Discussion, Action, Representation and Thought (DART) Board
23	Transport (government)	Connex
24	Private security industry	Inner Range; Australian Security Industry Association Ltd; Southern Health; Victorian Security Advisory Committee; SMI Security Group, ADT Security; Siemens Security
25	Private investigation industry	Victorian Detective Services; Maurice J Kerrigan and Associates; Institute of Mercantile Agents
26	Print media	Herald and Weekly Times; Leader Newspapers; Australian Press Council; Australian Commercial and Media Photographers; Australian Photographic Society
27	Electronic media and legal firms	Holding Redlich; Corrs Chambers Westgarth; Minter Ellison; Victorian College of the Arts; Film and Television School; ABC News and Current Affairs; Channel 10 News; Commercial Radio Australia; Communications Law Centre; Australian Subscription Television and Radio Association
28	Indigenous community groups	Regional Aboriginal Justice Advisory Committee; Indigenous Issues Unit, Department of Justice
29	Insurance agencies	ANZ Bank
30	Crime Stoppers Victoria	Crime Stoppers Victoria
31	Property Councils	Centro Properties Group; Property Council of Australia

Bibliography

- Adams, Dan, 'Climate Change and Human Rights' (Paper presented at the '2008 Human Rights Oration', Victorian Equal Opportunity and Human Rights Commission, Melbourne, 10 December 2008)
- Alzheimer's Australia, 'Safer Walking for People with Dementia: Approaches and Technologies', Update Sheet No 16 (2009)
- Arjoon, Surendra, 'Striking a Balance Between Rules and Principle-Based Approaches for Effective Governance: A Risks-Based Approach' (2006) 68(1) *Journal of Business Ethics* 53
- Attorney-General's Department, Australian Government, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007)
- Australian Communications and Media Authority, *Privacy Guidelines for Broadcasters* (2005)
- Australian Government, *Enhancing National Privacy Protection: First Stage Response to the Australian Law Reform Commission Report 108: For Your Information: Australian Privacy Law and Practice* (2009)
- Australian Institute of Criminology, *Considerations for Establishing a Public Space CCTV Network*, Research in Practice No 8 (2009)
- Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 1: Final Report 108* (2008)
- Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 2: Final Report 108* (2008)
- Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice: Volume 3: Final Report 108* (2008)
- Australian Law Reform Commission, *Principled Regulation: Federal Civil and Administrative Penalties in Australia*, Report No 95 (2002)
- Australian Law Reform Commission, *Privacy*, Report No 22 (1983)
- Ayres, Ian and Braithwaite, John, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press, 1992)
- Baldwin, Robert and Black, Julia, *Really Responsive Regulation*, Law Society Economy Working Paper No 15/2007 (London School of Economics and Political Science, 2007)
- Black, Julia, 'Managing Discretion' (Paper presented at the Australian Law Reform Commission Conference, Penalties: Policy, Principles and Practice in Government Regulation, Sydney, 7 June 2001)
- Black, Julia, Hopper, Martyn and Band, Christa, 'Making a Success of Principles Based Regulation' (2007) 1(3) *Law and Financial Markets Review* 191
- Braithwaite, John, 'Rewards and Regulation' (2002) 29(1) *Journal of Law and Society* 12
- Briefing 15.12.09: National CCTV Oversight Body* National CCTV Strategy Board, Home Office <www.crimereduction.homeoffice.gov.uk/cctv/cctv_oversight_body_b.pdf> at 20 January 2010
- British Columbia Law Institute, *Report on the Privacy Act of British Columbia*, BCLI Report No 49 (2008)
- Budde, Paul, *Australia: Mobile Communications Subscriber Statistics* (2004) <www.budde.com.au/Research/Australia-Mobile-Communications-Subscriber-Statistics.html> at 5 March 2005
- Burrows, John, 'Privacy and the Courts' (Paper presented at the Privacy Forum, Wellington, New Zealand, 27 August 2008)
- Butler, Des, 'A Tort of Invasion of Privacy in Australia' (2005) 29 *Melbourne University Law Review* 339
- Callinan, Ian, 'Privacy, Confidence, Celebrity and Spectacle' (2007) 7 *Oxford University Commonwealth Law Journal* 1
- Cameron, Alex and Palmer, Mimi, 'Invasion of Privacy as a Common Law Tort in Canada' (2009) 6(11) *Canadian Privacy Law Review* 105
- Chester, Simon, Murphy, Jason and Robb, Eric, 'Zapping the Paparazzi: Is the Tort of Privacy Alive and Well?' (2003) 27 *Advocates' Quarterly* 357
- Clarke, Roger, 'You Are Where You've Been: Location Technologies' Deep Privacy Impact' (Paper presented at the You Are Where You've Been: Technological Threats to Your Location Privacy Seminar, Sydney, 23 July 2008)
- Coleman, Clive and Norris, Clive, *Introducing Criminology* (Willan Publishing, 2000)
- College Bescherming Persoonsgegevens, *If You Record People on Video Camera*, Fact Sheet No 20A (2005)
- College Bescherming Persoonsgegevens, *If You are Recorded by a Video Camera*, Fact Sheet No 20B (2005)

- Crime Prevention and Community Safety and Tasmania Police, *Evaluation of the Devonport CCTV Scheme* (2002)
- Crisci, Camrin, '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
- Dean, Robert, 'Sex, Videotape and the Law' (2009) 83(8) *Law Institute Journal* 52
- Department of Justice (Victoria), *An Equality Act for a Fairer Victoria: Equal Opportunity Review, Final Report* (2008)
- Department of Justice (Victoria), *Attorney-General's Justice Statement 2: The Next Chapter* (2008)
- Department of Sustainability and Environment, *Victoria's Environmental Sustainability Framework: Our Environment Our Future* (2005) <www.dse.vic.gov.au/DSE/nrence.nsf/LinkView/C50F9AEFF496CEA8CA256FE800232FE1E2176767455B21FFCA256E57007C82CF> at 8 December 2005
- 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)
- Eady, Justice David, Speech delivered at the University of Hertfordshire, 10 November 2009 <www.judiciary.gov.uk/docs/speeches/justice-eady-univ-of-hertfordshire-101109.pdf> at 20 April 2010
- Edmond, Gary et al, 'Law's Looking Glass: Expert Identification Evidence Derived from Photographic and Video Images' (2009) 20 *Current Issues in Criminal Justice* 337
- Electronic Privacy Information Centre and Privacy International, *Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments* (2007)
- Equal Opportunity for Women in the Workplace Agency, *Annual Report 2008–2009* (2009)
- 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) No L 281 *EN: Official Journal of the European Communities* 31
- Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 1–3: Advice to Agencies about Collecting Personal Information* (1994)
- Fenwick, Helen and Phillipson, Gavin, *Media Freedom Under the Human Rights Act* (Oxford University Press, 2006)
- Fisse, Brent and Braithwaite, John, *The Impact of Publicity on Corporate Offenders* (State University of New York Press, 1983)
- Fleming, John, *The Law of Torts* (9th ed) (LBC Information Services, 1998)
- Ford, Harold, Austin, R P and Ramsay, Ian, *Ford's Principles of Corporations Law* (13th ed, LexisNexis Butterworths, 2007)
- Foucault, Michel, *Discipline and Punish: The Birth of the Prison* (Random House, 1975)
- George, Patrick, *Defamation Law in Australia* (LexisNexis Butterworths, 2006)
- Gill, Martin and Spriggs, Angela, *Assessing the Impact of CCTV*, Home Office Research Study 292 (Home Office, 2005)
- Gilliom, John, *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy* (University of Chicago Press, 2001)
- Goold, Benjamin, *CCTV and Policing* (Oxford University Press, 2004)
- Goold, Benjamin, 'Open to All? Regulating Open Street CCTV and the Case for "Symmetrical Surveillance"' (2006) 25(1) *Criminal Justice Ethics* 3
- Gras, Marianne, 'The Legal Regulation of CCTV in Europe' (2004) 2(2/3) *Surveillance & Society* 216
- Greenleaf, Graham, 'Global Protection of Privacy in Cyberspace—Implications for the Asia-Pacific' (Paper presented at the Internet Law Symposium, Taiwan, 23–24 June 1998)
- Haggerty, Kevin and Ericson, Richard, 'The Surveillance Assemblage' (2000) 51(4) *British Journal of Sociology* 605
- Hempel, Leon and Töpfer, Eric, *CCTV in Europe: Final Report* (Urbaneye, 2004)
- Home Office Police Department, *Closed Circuit Television in Public Places: Its Acceptability and Perceived Effectiveness*, Report 35 (1992)
- Human Rights Committee, *General Comment 16 (Twenty-Third Session, 1988) Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies* UN Doc HRI/GEN/Rev.6 at 142 (2003)
- Human Rights Unit, Department of Justice (Victoria), *Charter of Human Rights and Responsibilities: Guidelines for Legislation and Policy Officers in Victoria* (2008)

Bibliography

- 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 4 March 2009
- Joseph, Sarah, Schultz, Jenny and Castan, Melissa, *The International Covenant on Civil and Political Rights: Cases, Materials and Commentary* (2nd ed, Oxford University Press, 2004)
- Keeton, W Page et al (eds), *Prosser and Keeton on the Law of Torts* (5th ed, West Publishing, 1984)
- Kenyon, Andrew and Richardson, Megan (eds), *New Dimensions in Privacy Law: International and Comparative Perspectives* (Cambridge University Press, 2006)
- Koskela, Hille, "'Cam Era"—The Contemporary Urban Panopticon' (2003) 1(3) *Surveillance & Society* 292
- Law Reform Commission (Ireland), *Privacy: Surveillance and the Interception of Communications*, LRC 57–1998 (1998)
- Law Reform Commission of Hong Kong, *Privacy: The Regulation of Covert Surveillance*, Report (2006)
- Ludlow, Christa, "'The Gentlest of Predations": Photography and Privacy Law' (2006) 10 *Law Text Culture* 135
- Lyon, David, *Surveillance Society: Monitoring Everyday Life* (Open University Press, 2001)
- Lyon, David, *Surveillance Studies: An Overview* (Polity Press, 2007)
- Mason, Anthony, 'Legislative and Judicial Law-Making: Can We Locate an Identifiable Boundary' (2003) 24 *Adelaide Law Review* 15
- McClurg, Andrew, 'Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places' (1995) 73 *North Carolina Law Review* 989
- McNairn, Colin and Scott, Alexander, *Privacy Law in Canada* (Butterworths, 2001)
- Melbourne Centre for Criminological Research and Evaluation for Corrections Victoria, Department of Justice, *Home Detention in Victoria: Final Evaluation Report* (2006)
- Mendelson, Danuta, *The New Law of Torts* (Oxford University Press, 2007)
- Mendelson, Danuta, 'Illusionary Rights to Confidentiality and Privacy in the 21st Century?' (Paper presented at Deakin University, Melbourne, 26 August 2009)
- Metlink Melbourne, *Victorian Fares and Ticketing Manual (Myki)* (2009) <www.metlinkmelbourne.com.au/fares-tickets/victorian-fares-and-ticketing-manual-myki/> at 23 November 2009
- Michael, Katrina, MacNamee, Andrew and Michael, M G, 'The Emerging Ethics of Humancentric GPS Tracking and Monitoring' (Paper presented at the International Conference on Mobile Business: IEEE Computer Society, Copenhagen, Denmark, 25–27 July 2006) <ro.uow.edu.au/cgi/viewcontent.cgi?article=1384&context=infopapers> at 21 May 2008
- Moran, Eamonn, 'Enforcement Mechanisms (including Alternatives to Criminal Penalties)' (2009) 2 *The Loophole* 12
- Moreham, Nicole, 'Privacy in Public Places' (2006) 65 (3) *Cambridge Law Journal* 606
- Morrison, David and Svennevig, Michael, 'The Defence of Public Interest and the Intrusion of Privacy' (2007) 8(1) *Journalism* 44
- Mulheron, Rachel, 'Exemplary Damages and Tort: An International Comparison' (2000) 2 *University of Notre Dame Australia Law Review* 17
- Mullaly, Jennifer, 'Privacy: Are the Media a Special Case?' (1997) 16(1) *Communication Law Bulletin* 10
- NSW Law Reform Commission, *Surveillance: An Interim Report*, Report 98 (2001)
- NSW Law Reform Commission, *Surveillance: Final Report*, Report 108 (2005)
- NSW Law Reform Commission, *Invasion of Privacy*, Consultation Paper 1 (2007)
- NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009)
- New Zealand Law Commission, *Privacy: Concepts and Issues: Review of the Law of Privacy: Stage 1*, Study Paper 19 (2008)
- New Zealand Law Commission, *Invasion of Privacy: Penalties and Remedies Review of the Law of Privacy: Stage 3*, Issues Paper 14 (2009)
- New Zealand Law Commission, *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy: Stage 3*, Report 113 (2010)
- Norris, Clive and Armstrong, Gary, *The Maximum Surveillance Society: The Rise of CCTV* (Berg, 1999)

- Nouw, Sjaak, Vries, de Berend and Prins, Corien (eds), *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy* (T-M-C-Asser Press, 2005)
- Office of the Data Protection Commissioner (Ireland), *What Issues Surround the Use of CCTV* <www.dataprotection.ie/viewdoc.aspx?DocID=642> at 19 January 2009
- Offices of the Federal Privacy Commissioner and Human Rights and Equal Opportunity Commission, *Covert Surveillance in Commonwealth Administration: Guidelines* (1992)
- Office of the Federal Privacy Commissioner, *The Operation of the Privacy Act Annual Report, 1 July 2008–30 June 2009* (2009)
- 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) <www.privcom.gc.ca/information/guide/vs_060301_e.asp> at 4 March 2009
- Office of the Victorian Privacy Commissioner, *Annual Report 2008–2009* (2009)
- Office of the Victorian Privacy Commissioner, *Images and Privacy*, Info Sheet 1.03 (2003)
- Office of the Victorian Privacy Commissioner, *Jenny's Case: Report of an Investigation into the Office of Police Integrity Pursuant to Part 6 of the Information Privacy Act 2000*, Report 01.06 (2006)
- Office of the Victorian Privacy Commissioner, *Mobile Phones with Cameras*, Info Sheet 05.03 (2003)
- Office of the Victorian Privacy Commissioner, *Model Terms for Transborder Data Flows of Personal Information*, Guidelines Edition.01 (2006)
- Office of the Victorian Privacy Commissioner, *Mr C's Case: Report of an Investigation Pursuant to Part 6 of the Information Privacy Act 2000 into Victoria Police and Department of Justice in Relation to the Security of Personal Information in the Law Enforcement Assistance Program (LEAP) and E* Justice Databases*, Report 03.06 (2006)
- Office of the Victorian Privacy Commissioner, *Privacy and Global Positioning System Technology*, Info Sheet 2.08 (2008)
- Office of the Victorian Privacy Commissioner, *Short Guide to the Information Privacy Principles* (2006)
- Office of the Victorian Privacy Commissioner, *Who's Covered by the Information Privacy Act?* Info Sheet 01.06 (2006)
- Painter, Kate and Tilley, Nick (eds), *Surveillance of Public Space: CCTV, Street Lighting and Crime Prevention* (Criminal Justice Press, 1999)
- Parker, Christine, 'Reinventing Regulation within the Corporation: Compliance-Oriented Regulatory Innovation' (2000) 32(5) *Administration and Society* 529
- Parliamentary Travelsafe Committee, Queensland Parliament, *Report on the Inquiry into Automatic Number Plate Recognition Technology*, Report No 51 (2008)
- Posner, Richard, 'The Right of Privacy' (1978) 12(3) *Georgia Law Review* 393
- Privacy Commissioner (New Zealand), *Privacy and CCTV: A Guide to the Privacy Act for Businesses, Agencies and Organisations* (2009) <www.privacy.org.nz/privacy-and-cctv-a-guide-to-the-privacy-act-for-businesses-agencies-and-organisations/> at 26 October 2009
- Privacy Commissioner (New Zealand), *Privacy and CCTV: A Guide to the Privacy Act for Businesses, Agencies and Organisations* (2009) <www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/Privacy-and-CCTV-A-guide-October-2009.pdf> at 26 October 2009
- Privacy Commissioner (New Zealand), 'Tracking Technology on the Move' (2005) 54 *Private Word* 1
- Prosser, William, 'Privacy' (1960) 48(3) *California Law Review* 383
- Queensland Government Response to the Parliamentary Select Committee on Travelsafe's Report No 51: *Report on the Inquiry into Automatic Number Plate Recognition Technology* (2009) <<http://www.parliament.qld.gov.au/view/legislativeAssembly/tableOffice/documents/TabledPapers/2009/5309T434.pdf>> at 9 March 2010
- Ricketson, Sam, 'Public Interest and Breach of Confidence' (1979) 12 *Melbourne University Law Review* 176
- Riley, Tom et al, 'Implementing Advanced Image Processing Technology in Sensor Systems for Security and Surveillance' in *Proceedings of SPIE—The International Society for Optical Engineering: Volume 6741*, (2007)
- Rizos, Chris, 'Location Based Services and Issues such as Privacy' (Paper presented at the You are Where You've Been: Technological threats to Your Location Privacy Seminar, Sydney, 23 July 2008)
- Rizos, Chris, 'You are Where You've Been: Location Technologies' Deep Privacy Impact' (Paper presented at the You are Where You've Been: Technological Threats to Your Location Privacy Seminar, Sydney, 23 July 2008)

Bibliography

- Scassa, Teresa et al, 'Consumer Privacy and Radio Frequency Identification Technology' (2005–06) 37 *Ottawa Law Review* 215
- Select Committee on the Constitution, House of Lords, *Surveillance: Citizens and the State: Report*, Volume 1: 2nd Report of Session 2008–09 (2009)
- Shearmur, Jeremy, 'Free Speech, Offence and Religion' (2006) 22(2) *Policy* 21
- Siebel, Walter and Wehrheim, Jan, 'Security and the Urban Public Sphere' (2006) 3(1) *German Policy Studies* 19
- Slobogin, Christopher, 'Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity' (2002) 72 *Mississippi Law Journal* 213
- Solove, Daniel, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087
- Solove, Daniel, 'A Taxonomy of Privacy' (2006) 154(3) *University of Pennsylvania Law Review* 477
- Solove, Daniel, "'I've Got Nothing to Hide" and Other Misunderstandings of Privacy' (2007) 44 *San Diego Law Review* 745
- Solove, Daniel, *Understanding Privacy* (Harvard University Press, 2008)
- Spigelman, James, 'The Forgotten Freedom: Freedom from Fear' (Paper presented at the Sydney Law School, University of Sydney 17 November 2009 and Australian Academy of Law, Banco Court, Sydney, 18 November 2009)
- Standing Committee of Attorneys-General, *Unauthorised Photographs on the Internet and Ancillary Privacy Issues*, Discussion Paper (2005)
- Stapleton, Timothy, 'The Electronic Communications Privacy Act and Cell Location Data Is the Whole More than the Sum of its Parts?' (2007) 73(1) *Brooklyn Law Review* 383
- Surveillance Studies Network, *A Report on the Surveillance Society* (2006)
- Sutton, Adam and Wilson, Dean, 'Open-Street CCTV in Australia: The Politics of Resistance and Expansion' (2004) 2(2/3) *Surveillance & Society* 310
- Thompson, Mike, 'Biometrics: The Good, the Bad and the Ugly' (Paper presented at the Privacy Victoria How Do I Know Who You Are? Conference, Melbourne, 12 November 2008)
- Toulson, Roger, 'Freedom of Expression and Privacy' (2007) 41 *Law Teacher* 139
- United Kingdom Government, *Response to the House of Lords Selection Committee on the Constitution's Report: Surveillance: Citizens and the State* (2009)
- van den Hengel, Anton, Dick, Anthony and Hill, Rhys, *Activity Topology Estimation for Large Networks of Cameras* Australian Centre for Visual Technologies <www.acvt.com.au/research/surveillance/AVSS06.pdf> at 1 October 2009
- Victoria Police, *Inquiry into Automatic Number Plate Recognition Technology (Submission)* (2008) <www.parliament.qld.gov.au/tsafe/view/historical/documents/committees/TSAFE/inquiry/ANPR%20technology/Submissions/14.pdf> at 14 January 2010
- Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005)
- Victorian Law Reform Commission, *Surveillance in Public Places*, Consultation Paper 7 (2009)
- Wakefield, Alison, 'The Public Surveillance Functions of Private Security' (2004) 2(4) *Surveillance & Society* 529
- Wallis Consulting Group, *Community Attitudes to Privacy 2007: Prepared for Office of the Privacy Commissioner*, Reference No WG3322 (2007)
- Ward, Matt, van Kranenburg, Rob and Backhouse, Gaynor, *RFID: Frequency, Standards, Adoption and Innovation* (2006) JISC Technology and Standards, Watch <www.jisc.ac.uk/whatwedo/services/techwatch/reports/horizonscanning/hs0602.aspx> at 11 November 2008
- Warren, Samuel and Brandeis, Louis, 'The Right to Privacy' (1890) 4(5) *Harvard Law Review* 194
- Wells, Helene, Allard, Troy and Wilson, Paul, *Crime and CCTV in Australia: Understanding the Relationship* (Bond University Press, 2006)
- Welsh, Brandon and Farrington, David, *Crime Prevention Effects of Closed Circuit Television: A Systematic Review*, Home Office Research Study 252 (Home Office, 2002)
- 'Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators' (2004) 18(1) *Harvard Journal of Law & Technology* 307
- Wilson, Dean and Sutton, Adam, *Open-Street CCTV in Australia* (Australian Institute of Criminology, 2003)
- Working Group on Privacy, Ireland, *Report of the Working Group on Privacy* (2006)