**Contents**

Preface 5
Terms of reference 6
Glossary 7
Executive summary 11
Recommendations 15

**Chapter 1: Introduction**

Introduction 19
Background 20
Important definitions 21
What is surveillance? 21
What is a public place? 22
Coverage of this report 22
Federal areas of concern 22
State law enforcement 23
Practices covered by information privacy laws 23

Other law reform activity 24
Australian Law Reform Commission 24
NSW Law Reform Commission 24
New Zealand Law Commission 25
UK House of Lords Select Committee 25
Hong Kong Law Reform Commission 26
Law Reform Commission of Ireland 26

Our process 26
Consultation Paper 26
Final Report 26

Outline of this report 27

**Chapter 2: Use of Surveillance in Public Places** 29

Introduction 30
Surveillance technology 31
Closed-circuit television (CCTV) 31
GPS and satellite technology 31
Tracking mobile phones 31
Radio frequency identification (RFID) 31
Automatic number plate recognition (ANPR) 31
Body imaging devices and scanners 32
Biometric technologies 32
Google Earth and Google Streetview 32

Major users of public place surveillance 32
Victoria Police 32
Corrections Victoria 34
Local councils 34
Public housing 35
Universities and TAFEs 35
Transport 35
Major public events: concerts and sports 38
Crown Casino 39
The hospitality industry 40
Shopping centres and retailers 40
The media 41
Marketing companies 41
Private investigators 41
Public and private insurers 42
The private security industry 42
Aged care 42
Personal uses 42

Conclusion 43

**Chapter 3: Current Law** 45

Introduction 46
Surveillance devices legislation 46
Information privacy legislation 47
Information privacy laws and public place surveillance 48
Enforcement of information privacy laws 49

Regulation of specific aspects of public place surveillance 50
Common law protections 51
The Victorian Charter of Human Rights and Responsibilities 51
Limits on the right to privacy under the Charter 52
Non-binding guidelines, standards and policies 52
Regulation in other jurisdictions 53
Other Australian jurisdictions 53
Other countries 54

Conclusion 54
Table 1: Legislation and binding codes relating to public place surveillance in Victoria 55
Table 2: Major non-binding instruments relating to public place surveillance in Victoria 57
Chapter 4: A Balanced Approach to Regulation

Introduction
The impact of public place surveillance

Benefits
Investigation of criminal activity and fraud
Asset protection and deterrence of crime
Safety
Operational needs
Managing the movement and conduct of people
News gathering and the dissemination of information
Artistic purposes, entertainment and other personal uses

Risks
Threat to privacy
Social exclusion
Loss of anonymity
The chilling effect
Criminal conduct and offensive uses
Publication on the internet
Surveillance may not work
Converging devices

A balanced approach to regulation
The Victorian Charter of Human Rights and Responsibilities
Regulatory theory

An overview of our recommendations and our approach
Conclusion

Chapter 5: Promoting Responsible Use of Surveillance in Public Places

Introduction
Principles to govern the use of surveillance in public places
Six public place surveillance principles
An independent regulator of public place surveillance
Regulatory functions
Encouraging responsible practice
Research and monitoring
Educating, providing advice and promoting understanding of laws and best practice
Developing and publishing best practice guidelines

Significant surveillance users: ensuring responsible practice
Significant users of public place surveillance
Reviewing advice prepared by significant users of public place surveillance
Examining the practices of significant users of public place surveillance
Advising of a significant user's failure to comply
Reporting to parliament
Investigations and proceedings in relation to SDA breaches
The most appropriate body to regulate public place surveillance
Relationship with other surveillance regulators
Review of Victoria Police surveillance practices
Regulatory features not recommended at this stage
Registration or licensing of some surveillance users
A complaint-handling power for the regulator
General own-motion investigatory powers
Procurement standards as a tool to encourage compliance

Conclusion
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
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
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).
<p>| <strong>Automatic number plate recognition (ANPR)</strong> | Technology that recognises symbols in images of a number plate and stores or uses those symbols to identify the vehicle. |
| <strong>Biometric surveillance</strong> | Surveillance conducted using biological data, for example, fingerprints, iris patterns or facial features. |
| <strong>Bluetooth</strong> | A wireless form of transmission that uses radio waves to transmit information over short distances. |
| <strong>Breach of confidence</strong> | When confidential information is disclosed to a wider audience. May result in a right to sue. |
| <strong>Cause of action</strong> | A right to sue another person. |
| <strong>CCTV</strong> | Closed-circuit television. Now a generic term for surveillance camera systems. |
| <strong>Chilling effect</strong> | Where speech or conduct is suppressed because of a belief that it may result in undesirable consequences. |
| <strong>Citizen journalism</strong> | Journalism undertaken by non-professionals. |
| <strong>Civil penalty</strong> | 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. |
| <strong>Common law</strong> | Law that derives its authority from the decisions of courts, rather than from Acts of parliament. |
| <strong>Convergence</strong> | When used in relation to technology, describes the phenomenon in which technology is becoming increasingly interconnected and multi-functional. |
| <strong>CrimTrac</strong> | A Commonwealth agency that uses, develops, and provides access to information technology and services for police use. |
| <strong>Data mining</strong> | The process of analysing data for known and unknown data patterns. |
| <strong>Data surveillance</strong> | The monitoring of data, as opposed to people or places. |
| <strong>Enforcement pyramid</strong> | A regulatory model characterised by increasing levels of intervention that utilises serious measures only when milder sanctions (such as education) have failed. |
| <strong>e-tag</strong> | A device attached to a vehicle that transmits information to an electronic reader; used to identify the vehicle for tolling purposes. |
| <strong>E-view (Enterprise view)</strong> | A web-based tool that provides detailed, zoomable images of buildings and other features compiled through aerial photographs. |
| <strong>Facial recognition</strong> | 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. |
| <strong>Global positioning system (GPS)</strong> | A navigation system that relies on information received from a network of satellites to provide the latitude and longitude of an object or location. |
| <strong>Google Earth</strong> | A web-based program that maps the earth by the superimposition of images obtained from satellite imagery and aerial photography. |
| <strong>Google Street View</strong> | 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. |
| <strong>Happy slapping</strong> | The practice of recording an assault on a victim (commonly with a camera phone) for entertainment. |
| <strong>In-car video</strong> | 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. |
| <strong>International Covenant on Civil and Political Rights (ICCPR)</strong> | A treaty giving effect to civil and political rights contained in the Universal Declaration of Human Rights. Australia is a signatory to the ICCPR. |
| <strong>Location surveillance</strong> | Identifying a person’s or an object’s whereabouts at a particular time. |
| <strong>Mass surveillance</strong> | Monitoring the public at large, or a significant part of the public, instead of a particular individual. |
| <strong>Nuisance</strong> | 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. |
| <strong>Optical character recognition</strong> | Software designed to recognise letters and numbers from a captured image and to translate them into editable text. |
| <strong>Optical surveillance</strong> | See Visual surveillance. |
| <strong>Own-motion investigation</strong> | The power of a regulator to investigate possible breaches of a law without the need for a complaint or referral by a person. |
| <strong>Olfactory surveillance</strong> | Purposeful monitoring of a person or object by smell, including by the use of a device or animal. |
| <strong>Panopticon</strong> | 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. |
| <strong>Participant monitoring</strong> | Recording of conversations or activities by someone participating in them. |</p>
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Passive location services</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Physical surveillance</strong></td>
<td>Observing a person by being physically present at their location.</td>
</tr>
<tr>
<td><strong>Profiling</strong></td>
<td>When used in a law enforcement context, reliance on personal traits (such as race, gender and age) to target potential offenders.</td>
</tr>
<tr>
<td><strong>Purpose creep</strong></td>
<td>In a surveillance context, where a surveillance system set up for one purpose is used for another purpose. Also known as ‘function creep’.</td>
</tr>
<tr>
<td><strong>Radio frequency identification (RFID)</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Text message/SMS</strong></td>
<td>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).</td>
</tr>
<tr>
<td><strong>SmartGate</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Smart card</strong></td>
<td>A card containing integrated circuits that can store and process data. Used for performing financial transactions and accessing restricted areas.</td>
</tr>
<tr>
<td><strong>Snaparazzi</strong></td>
<td>A play on the word ‘paparazzi’; used to describe the collection of unstaged and/or candid photographs of celebrities by non-professionals.</td>
</tr>
<tr>
<td><strong>Spyware</strong></td>
<td>Software that, once installed in a computer, secretly collects information about the computer use.</td>
</tr>
<tr>
<td><strong>Statute</strong></td>
<td>A written law passed by parliament.</td>
</tr>
<tr>
<td><strong>Surveillance</strong></td>
<td>Deliberate or purposive observation or monitoring of a person, object or place.</td>
</tr>
<tr>
<td><strong>Tort</strong></td>
<td>A breach of a duty, imposed by law, that protects the bodily integrity, property, reputation or other interests of a person.</td>
</tr>
</tbody>
</table>
### Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracking</td>
<td>Monitoring a person or object’s whereabouts over a period of time. Also called ‘location surveillance’.</td>
</tr>
<tr>
<td>Trespass</td>
<td>Direct interference with a person, goods, or property of another without lawful justification. May result in a right to sue.</td>
</tr>
<tr>
<td>Universal Declaration of Human Rights (UDHR)</td>
<td>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.</td>
</tr>
<tr>
<td>Upskirting</td>
<td>The observation or recording of a person’s genital or anal regions without their consent.</td>
</tr>
<tr>
<td>Visual surveillance</td>
<td>Purposeful monitoring of a person or object by sight, including by the use of a device. Also known as ‘optical surveillance’.</td>
</tr>
<tr>
<td>Voice over Internet Protocol (VoIP)</td>
<td>Generic term for technology that enables the delivery of voice communication over the internet and other networks.</td>
</tr>
<tr>
<td>Wire tapping</td>
<td>The use of electronic or mechanical equipment to gain access to transmission of private telephone conversations, computer data or facsimiles.</td>
</tr>
</tbody>
</table>
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.
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.
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:
17. 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.

18. 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.