Victorian
Law Reform
Commission

Privacy Law: Options For Reform
Information Paper

Victorian Law Reform Commission

GPO Box 4637
Melbourne 3001
Australia
DX 144 Melbourne

Level 10
10 – 16 Queen Street
Melbourne Victoria 3000
Australia

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

Contents

Contributors

Authors (in alphabetical order)**:** Tim Dixon, Michelle Fisher, Marcia Neave, Padma Raman Jamie Walvisch

Expert Advisory Committee

Mr Scott Beattie
Dr Breen Creighton
Mr Tim Dixon
Ms Victoria Marles
Mr Chris Maxwell QC
Ms Moira Paterson
Dr Barry Perry
Mr Nigel Waters

Victorian Law Reform Commission

Chairperson	Professor Marcia Neave AO
Chief Executive Officer	Padma Raman
Research and Policy Officers	Sara Charlesworth Stephen Farrow Michelle Fisher Ailsa Goodwin Jamie Walvisch
Research and Information Officer	Trish Luker
Operations Manager	Kathy Karlevski
Administrative Officers	Naida Jackomos Simone Marrocco Lorraine Pitman

Acknowledgments

The Victorian Law Reform Commission gratefully acknowledges advice and helpful comments on drafts provided by the Expert Advisory Committee. We also thank Tim Dixon for his assistance in writing this Paper.

Scope of this Information Paper

ATTORNEY-GENERAL'S REFERENCE

On 27 April 2001, the Attorney-General, The Honourable Rob Hulls, MP, asked the Victorian Law Reform Commission (the 'Commission') to examine the coverage of privacy protection in Victoria and advise on priority areas for reform. The Attorney-General said:

> *At the time of the last election, we made a policy commitment to law reform in the area of privacy and so I am pleased to announce that the first reference is to examine the coverage of privacy legislation for Victorians and to advise on priority areas for reform. For example, advances in technology have created a number of issues in the workplace in the use of the Internet. Another area of investigation might be around an individual's right to privacy in public places.*

PROCESS

The areas potentially covered by a review of privacy law in Victoria are broad and diverse. As part of the process of advising the Attorney-General on priority areas, the Commission has undertaken some preliminary research on current privacy law issues and has consulted with an Expert Advisory Committee.[1] The Commission is now seeking responses from privacy advocacy groups as part of the process of identifying priorities for law reform.

The Commission has not come to a settled view on priority areas for reform. The views set out in this Paper are tentative only and are intended to promote discussion about how the Commission should focus its work on privacy.

PURPOSE OF THIS PAPER

The aim of this Paper is to contribute to community debate on privacy law reform by providing information on existing privacy protection and highlighting gaps in the law. The focus of the research has been on ensuring that privacy rights are adequately protected.

STRUCTURE OF THIS PAPER

After briefly exploring the meaning of the right to privacy and discussing the challenges which new technologies pose to privacy protection (Chapter 1), this Paper examines five key dimensions of privacy which are recognised to some extent by the existing law. These laws affect:

- bodily privacy, by preventing unauthorised intrusions into a person's body, for example through DNA testing (Chapter 2);
- territorial privacy, by preventing unauthorised intrusions into a person's physical space, for example a home or business premises (Chapter 3);

[1] The members of this Committee are listed on p v.

- information privacy, by preventing unauthorised access to information held by government or private sector organisations, for example mailing lists and information contained on public registers such as the electoral roll (Chapter 4);

- communications privacy, by preventing unauthorised interception of private communications, for example telephone calls and emails (Chapter 5); and

- surveillance, by preventing unauthorised use of surveillance devices, for example video cameras in public and private places (Chapter 6).

A number of commentators have identified privacy in the workplace as posing particular problems for privacy protection.[2] This Paper therefore also specifically examines privacy in the workplace (Chapter 7), bringing together a number of the dimensions of privacy outlined above.

Throughout each of these Chapters we highlight the current legal protections offered for privacy in Victoria and note the gaps in that protection. We use a number of guiding principles to determine which of those areas the Commission's work might usefully focus upon. These principles include:

- whether investigation of the issue would involve duplicating work already being undertaken by other law reform bodies;

- whether the issue would be more appropriately dealt with at a Commonwealth level;

- whether existing privacy legislation has been in operation for a sufficient time for us to assess its impact; and

- the seriousness of the privacy problem which is being considered.

The Paper concludes by proposing the areas which the Commission believes may be priority areas for a reference on privacy law reform in Victoria (Chapter 8).

Please note that technical and legal terms are defined in the Glossary at the end of the Paper.

[2] This issue has been specifically highlighted by members of the Expert Advisory Committee and was reflected in a recent national conference on privacy: *Privacy Conference*, held in Melbourne on 25-26 June 2001.

Chapter 1
Privacy: Background

WHAT IS PRIVACY?

> *No-one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*[3]

1.1 'Privacy' is notoriously difficult to define, because it means different things to different people. It is an elusive concept because people's feelings about whether something should be kept private vary according to context. For example, they may be comfortable with friends knowing something about them, but may wish to prevent it coming to the knowledge of colleagues at work. The difficulty in defining privacy is compounded by the fact that views about what should be 'private' and what is 'public' vary between social groups, and what may be seen as privacy-intrusive behaviour in one society is quite acceptable in another. The notion of privacy also changes over time, sometimes as a result of individuals seeking to safeguard themselves against developments in technologies that may make it easier to obtain access to information about them, or which may make their behaviour more visible.

1.2 Although most people accept that certain areas of life should be private, there are disputes about the boundaries between what should be public and what should be private. Sometimes the idea of privacy has been used to justify failure to interfere with harmful behaviour such as domestic violence or child abuse, because it occurs in the 'private' area of the family.

1.3 In this paper we do not attempt the impossible task of producing a definitive definition of privacy. Instead we focus on the legal protection of some aspects of privacy. Despite the difficulties of defining the precise meaning of privacy,[4] international human rights conventions and treaties have recognised a right to privacy as a fundamental human right for many years.[5] The

---

[3] *International Covenant on Civil and Political Rights*, art 17(1).

[4] For a detailed discussion of the meaning and function of privacy, see Law Reform Commission of Hong Kong, Sub-committee on Privacy, 'Right to privacy', Chapter 1 in *Consultation Paper on Civil Liability for Invasion of Privacy*, August 1999, available at <http://www.info.gov.hk/hkreform/reports/privacy-e.htm>. We note that, in America, matters such as abortion, homosexuality and obscenity are often discussed as privacy matters. While these issues involve aspects of privacy, Australian debates around these areas have not been articulated in the context of privacy. In line with the nature of the debate in Australia this Paper does not examine these issues.

[5] See, eg, Universal Declaration of Human Rights 1948, art 12; International Covenant on Civil and Political Rights (ICCPR), art 17; Convention on the Rights of the Child, art 12. Some commentators discuss privacy in terms of interests rather than rights. Privacy expert Dr Roger Clarke, for example, defines privacy as 'the interest that individuals have in sustaining a "personal space", free from interference by other people or organisations'. See R Clarke, 'Introduction to Dataveillance and Information Privacy, and Definition of Terms' (1999) <http://www.anu.edu.au/people/Roger.Clarke/DV/intro.html>. A 'right to privacy' is not explicitly recognised in Australian law. However, as demonstrated in this Paper, some aspects of the right are protected by common law and legislation.

concept of a right to privacy reflects the belief that individuals should be able to exercise control over their own lives and have some say in the extent to which other individuals, governments or corporations obtain access to information about them or intrude in their life in other ways. This was recognised by the Australian Law Reform Commission in its landmark 1983 report:

> Claims to privacy are part of the claim that the autonomy of each individual should be protected and his integrity respected. Privacy claims involve a number of aspects:
>
> - that the person of the individual should be respected, i.e. it should not be interfered with without consent;
>
> - that the individual should be able to exercise a measure of control over relationships with others; this means that:
>
> - a person should be able to exert an appropriate measure of control on the extent to which his correspondence, communications and activities are available to others in the community; and
>
> - he should be able to control the extent to which information about him is available to others in the community.[6]

1.4 Put at its simplest, the right to privacy is often defined as the 'right "to be let alone"'[7] – that is, the right to protect some aspects of personal life from the possible view or intrusion of others. This is necessary in order to preserve human dignity, enable and enhance personal growth, and allow meaningful relationships to be created and maintained. This right 'to be let alone', however, is not an absolute right. It involves balancing privacy with competing interests – for example, the interest of the community in freedom of speech or in the apprehension and conviction of people who have committed criminal offences.

DEVELOPMENT OF PRIVACY LAW

1.5 The notion of 'a right to privacy' is comparatively modern. In earlier times, people received some incidental privacy protection from laws providing remedies for assault and battery, nuisance and trespass to land and goods.[8] These laws gave some protection against physical intrusion into, or interference with, an individual's body or property but were not specifically focused on the protection of privacy.

1.6 Over time, privacy-related common law principles have developed and/or legislation has been enacted to deal with the implications of particular social or technological changes, such as the development of methods of mass communications such as newspapers[9] and the advent of

---

6 Australian Law Reform Commission, *Privacy* (1983) paras 1032, 1033.

7 Judge Cooley, *Cooley on Torts*, (2nd ed, 1888) 29, cited in Samuel Warren and Louis D. Brandeis, 'The Right to Privacy' (Dec 1890) 4 *Harvard Law Review* 193, available at: <http://www.louisville.edu/library/law/brandeis/privacy.html>.

8 Defamation laws which prevented the publication of false statements injuring a person's reputation also provided some incidental privacy protection.

9 The common law action of breach of confidence gives individuals some protection against the publication of confidential personal information. See, for example, *Argyll v Argyll* [1967] Ch 302; [1965] 1 All ER 611.

telephones.[10] While often the primary purpose of these laws has been to protect rights other than privacy they have incidentally provided some privacy protection.

1.7 In many countries privacy is now protected by constitutional guarantees or general human rights legislation.[11] In Australia, privacy receives more piecemeal protection. It was not until the 1980's that Australia first developed any privacy-specific legislation. In the 1980's and 1990's concerns about the privacy of personal information led to the enactment of Commonwealth and, later, State privacy legislation.[12] Both State and Commonwealth Governments have recently legislated to provide for broader privacy protection in relation to personal information.[13] In addition, as a result of the increasing use of surveillance technologies, State legislation has been enacted to regulate the use of surveillance devices.[14]

NEW CHALLENGES

1.8 The social and technological changes of the early 21st century create challenges to privacy on an unprecedented scale. The convergence of information and communications technology, combined with new approaches to management and industrial relations, have created increasing risks of privacy infringements. In the past concerns about privacy infringements often related to the actions of government. Today they are as likely to focus on the activities of the media, large corporations and small businesses.

1.9 The use of new technologies by government, individuals and private sector organisations has an impact on all the aspects of privacy identified in this Paper. Bodily and territorial privacy is affected by developments in biometrics,[15] genetics, surveillance and tracking technologies. Privacy of communications is challenged by the availability of scanning and surveillance devices. Both information and communications privacy are threatened by the fact that more information can now be collected about individuals than ever before, including every telephone call, credit card purchase and communication by email. Never before has so much information been generated on the lives of ordinary individuals and never has it been so easy and cheap to send that

---

[10] The advent of telephones resulted in the enactment of legislation protecting the privacy of telecommunications: See 20 Vic. No. 41, *An Act to establish and regulate Electric Telegraphs 1957* (NSW), s 9; 21 Vic. No. 6. *An Act to regulate the construction and management of Electric Telegraphs 1857* (SA), s 9; 20 Vic. No. 22, *The Electric Telegraph Act 1857* (Tas), s. 11; 55 Vic. No. 15, *The Post and Telegraph Act 1891* (Qld), s 7 and Third Schedule.

[11] Countries that recognise a right to privacy within their Constitution range from the Kingdom of the Netherlands (*Constitution of the Kingdom of the Netherlands 1989*) to the Republic of the Philippines (art III, *Constitution of the Republic of the Philippines 1987*) to the Russian Federation (art 23, *Constitution of the Russian Federation* 1993 available at <http://www.friends-partners.org/oldfriends/constitution/russian-const-ch2.html>). While the Constitution of the United States of America does not contain an explicit right to privacy, the Courts going back as far as 1891 (*Union Pacific R.R. Co. v. Botsford*, 141 U.S. 251 11 S.Ct. 1000, 35 L.Ed. 734(1891))have interpreted the Constitution as providing a right to personal privacy: see *Roe v Wade* 410 U.S. 113, 93 S.Ct. 705, 35 L.Ed.2d 147. An example of a country that has recently enacted general human rights legislation that protects the right to privacy is the United Kingdom: *Human Rights Act 1998* (UK).

[12] This is discussed in more detail in Chapter 4.

[13] *Information Privacy Act 2000* (Vic) and *Privacy Amendment (Private Sector) Act 2000* (Cth).

[14] *Surveillance Devices Act 1999* (Vic). New South Wales have enacted legislation specifically regulating surveillance in the workplace: *Workplace Video Surveillance Act 1998* (NSW). These Acts are discussed in more detail in Chapter 6.

[15] 'Biometrics' involves the measurement of biological phenomena, through methods such as fingerprinting, thumb scanning, hand geometry, retina scanning and voice recognition.

information around the world. Much of this information is the trivia of daily life but taken out of context this kind of information can easily embarrass or disadvantage a person.

1.10 The legal systems of developed countries have struggled to keep up with the speed with which these technologies are being developed and applied. In Australia, privacy laws still provide individuals only piecemeal and haphazard protection. At the same time as new technologies are resulting in the need to provide greater protection, they are also undermining the effectiveness of national regulation. New technologies rapidly break down the barriers between countries making it harder for national governments to put safeguards in place. Governments have already found that Internet websites which are banned because of their content may simply move offshore. Similar problems arise in regulating electronic privacy invasions which may occur outside Australia. Governments may also find that proposed measures to protect privacy meet the staunch opposition of business interests which see such safeguards as an expense and an unjustified constraint on their right to conduct their business affairs.[16]

1.11 The inadequacy of current privacy laws in addressing these new challenges was summed up by the Director-General of the global advocacy organisation Privacy International:

> *We have a privacy law, but it is more or less useless as a tool to stall the surveillance juggernaut. We have a Privacy Commissioner, but he is little more than a government functionary... Talk to the experts in this field and you will be bombarded by legalities. With furrowed brows they will passionately outline conventions, legislation and regulations. They will lecture you on definitions, connotations and exemptions. You will listen, with growing bemusement, to how such and such an information practice breaches such and such a data protection principle and you will learn about how this may or may not be in contravention of so many other directives, codes or conventions. And in the end, you suddenly realise that these things hardly matter at all.*[17]

1.12 These comments highlight the importance of ensuring that privacy laws are capable of responding to changes in social attitudes and technological developments. It is in the context of such developments that the Commission seeks to determine appropriate areas for reform.

---

[16] For example, the United States is currently debating the merits of privacy legislation, and a major part of the debate concerns the costs to business. Robert Hahn, in a study supported by the Association for Competitive Technology, estimated in May 2001 that privacy regulation in the United States would impose costs of $US30bn on industry. The study is called 'An assessment of the Costs of the Proposed Online Privacy legislation' and is available at <http://www.actonline.org/pubs/HahnStudy.pdf>. An analysis of the report by Peter Swire, former White House Counsellor on Privacy, is highly critical of the methodology and argues that the cost estimations are not valid: see Peter Swire, 'New Study Substantially Overestimates Costs of Internet Privacy Protections', 9 May 2001, available at <http://www.osu.edu/units/law/swire1/pshome1.htm>.

[17] Simon Davies, *Monitor: Extinguishing Privacy on the Information Superhighway*, Pan Macmillan, Sydney 1996 pp 2, 6.

Chapter 2
Bodily Privacy

> *[A] claim to the privacy of one's person is protected by laws guaranteeing freedom of movement and expression, prohibiting physical assault, and restricting unwarranted search or seizure of the person. This notion … is spatial in the sense that the physical person is deemed to be surrounded by a bubble or aura protecting him from physical harassment. But, unlike physical property, this 'personal space' is not bounded by real walls or fences, but by legal norms and social values. Furthermore, this sense of privacy transcends the physical and is aimed essentially at protecting the dignity of the human person.*[18]

BACKGROUND

2.1 Bodily intrusion is arguably the most severe breach of privacy. It may take the form of a direct invasion of bodily integrity such as when a person is blood tested without their consent, or indirect physical intrusion through, for example, various forms of biometric testing which enable information to be obtained about a person's body without physical contact.[19] It may also be treated as including psychological intrusion, such as being required by one's employer to undergo regular personality testing.

2.2 Technological changes, including developments in medical science and biometric technology, are making intrusions into bodily privacy more common. Examples include:

- police taking DNA samples from suspects in criminal investigations and in some instances taking DNA samples from a wider population;
- security systems requiring biometric identification such as hand scanning to verify identity before providing access to a secure area for employees;
- sporting bodies performing drug tests on athletes;
- entertainment venues frisking people attending events;
- employers requiring extensive psychological testing from prospective employees;
- health agencies requiring blood tests from people suspected of carrying an infectious disease; and
- insurance agencies requiring bodily samples in order to conduct genetic testing.

---

[18] Department of Communications and Department of Justice, Canada, Privacy and Computers 1972, quoted in Australian Law Reform Commission, above n 6, para 47.

[19] Examples of biometric technologies that allow such indirect intrusions include voice and face recognition systems.

2.3 In certain circumstances some of these intrusions may be justified. However, the increasing use of these techniques raises important questions about the balance between privacy rights and other competing interests.

2.4 Intrusions into bodily privacy usually occur in order to obtain information about an individual. Many of the issues which arise in relation to the privacy of the body are therefore primarily concerned with the right of individuals to control the collection, use and disclosure of their personal information. As a result, protection of bodily privacy overlaps substantially with information privacy rights.[20] The focus of bodily privacy, however, is on the issue of whether an intrusion into the privacy of the body should occur in the first place, rather than on issues relating to the use and disclosure of personal information.

HOW IS BODILY PRIVACY PROTECTED

2.5 In Chapter 1 we discussed the fact that historically the law has protected bodily integrity by providing civil and criminal remedies for assault and battery, although privacy protection was not the primary purpose of these laws.[21]

2.6 In civil law, the wrong of battery is constituted by a direct interference with a person's body without their consent.[22] This includes interference ranging from 'frisking' a person without their consent to body cavity searches, unless such activities are authorised by law. A battery does not require physical contact between the perpetrator and the victim – an interference with a body by a weapon or instrument (such as a syringe) is sufficient.[23] There is no requirement that the interference be hostile[24] nor is it necessary for the individual to know of the interference. For example, a surgeon operating on an unconscious person could potentially commit battery.

2.7 A civil action for assault can arise when a person's actions lead another person to fear that there will be a direct physical interference with their body. People can recover monetary damages for a civil assault or battery.

2.8 Acts which constitute a civil assault or battery are also likely to be punishable as crimes. Relevant offences include common assault, intentionally or recklessly causing injury or serious injury and a variety of sexual offences.[25]

---

[20] These are discussed in detail in Chapter 4.

[21] As restraining a person's liberty can also be classified as an invasion of bodily privacy, legal actions for false imprisonment could also provide some protection.

[22] Remedies for indirect interferences with a person's body also exist (for example, providing someone with poisoned food, rather than actually feeding it to them): See, eg, *Bird v Holbrook* (1828) 4 Bing 628; 130 ER 911. As the issues arising in relation to bodily 'privacy' generally involve direct interference with the body we do not discuss indirect interferences in this Paper.

[23] *Pursell v Horn* (1838) 8 Ad & E 602; 112 ER 966.

[24] *Boughey v the Queen* (1986) 161 CLR 10.

[25] See, eg, *Crimes Act 1958* (Vic) ss 16–18 and 38–52.

WHAT ARE THE LIMITS ON LEGAL PROTECTION?

2.9 Existing legal remedies do not provide protection against intrusions which do not involve physical contact, or fear of physical contact, with the body. For example, it is not a battery to require a person to undergo psychological testing or to require them to undergo scanning as they enter a building.

2.10 If a person genuinely consents to an interference with their body there will also generally be no civil or criminal liability for the intrusion.[26] Such consent can be expressed by the person or implied from the circumstances. For example, a person may sign a consent form before being vaccinated by a doctor or they may simply cooperate with the vaccination by rolling up a sleeve. The law also presumes the existence of such consent in relation to 'everyday' physical contact such as bumping into someone on the train.[27]

2.11 Consent to a bodily intrusion will often be genuine as, for example, when a person allows a hairdresser to cut their hair. However, in some cases a person may feel that they cannot refuse consent. For example, some people have expressed concern about the increasing use of biometric devices in the workplace.[28] Although employees may be seen to consent to the use of such devices, this may be as a result of their overriding need to retain their job.

2.12 The law also allows interference with a person's body in some situations. For example, previously, at common law a person could arrest anyone found committing a breach of the peace in their presence, or a person who was reasonably suspected of having committed a felony. Police had wider powers of arrest.[29] There was, however, no common law power to invade a person's body – the police had no right to take fingerprints or blood samples without consent. In Victoria, the right to arrest people has now been codified in the *Crimes Act 1958* (Vic).[30] The police have also, over time, been given more extensive powers which allow them to intrude into a person's bodily privacy for investigative purposes. In particular circumstances the police can now conduct strip searches, body cavity searches, take fingerprints and take other body tissue samples to perform forensic procedures.[31]

2.13 Lawful intrusions into bodily privacy are not limited to the police. Other agencies that have powers to intrude into a person's bodily privacy in prescribed situations include customs,[32] corrections[33] and health agencies.[34]

---

[26] Consent may not be a defence to some bodily interferences, such as a battery that causes serious injury: see, eg, *Pallante v Stadiums Pty Ltd [No.1]* [1976] VR 331; *R v Brown* [1994] 1 AC 212.

[27] *Collins v Wilcock* [1984] 3 All ER 374.

[28] A Shulman, *Workplace: Employee Privacy*, Paper presented at Privacy Conference, Melbourne, 25 June 2001.

[29] A person who is arrested without legal authorisation can sue the other person for false imprisonment.

[30] See ss 457-463B.

[31] See, eg, *Crimes Act 1958* (Vic) ss 464K–ZK. It should be noted that while many of these provisions relate to the actual intrusion into the body, a number of them also provide protections for the information obtained from such intrusions – protecting 'information privacy'.

[32] See, eg, *Customs Act 1901* (Cth) ss 219L–ZL.

[33] See, eg, *Corrections Act 1986* (Vic) ss 28–29A, 45.

IS BODILY PRIVACY ADEQUATELY PROTECTED?

2.14 While laws providing remedies for assault and battery protect individuals from many forms of bodily interference, it is arguable that reforms are needed to protect people against intrusive conduct which is not adequately regulated. Questions relating to protection of bodily privacy include:

- Are people adequately protected against unauthorised invasions by the police?
- Are people adequately protected against unauthorised invasions by other investigatory authorities?
- Should there be legislative protection of genetic privacy?
- Is law reform needed to deal with new technologies such as biometrics and psychometrics?[35]

Each of these issues is briefly discussed below, together with some tentative views about the priorities for law reform in this area.

Police

2.15 As discussed above, police powers to intrude into people's bodies for investigative purposes have been expanded over time. Often the extent of these powers is not clearly defined, allowing for the possibility of abuse. For example, the *Crimes Act 1958* (Vic) does not specify the precise circumstances in which police can undertake strip searches.[36] In addition, as DNA identification technology improves police powers continue to expand.[37] It is arguable that with this expansion bodily privacy is not adequately protected and that further safeguards are necessary.

2.16 The current view of the Commission is that the issue of police powers raises civil liberty issues which extend beyond the scope of concerns about privacy. For this reason we do not propose that investigation of police powers should be treated as a priority area for the Commission's privacy reference.

Other investigatory authorities

2.17 Other investigatory authorities, such as the Transport Accident Commission and the WorkCover Authority, have also been given investigative powers to aid them in the performance of their functions and to help them ensure that they are not being defrauded. For example, a person seeking WorkCover benefits may be asked to submit to a medical examination. Although

---

[34] See, eg, *Health Act 1958* (Vic) s 121.

[35] 'Psychometrics' involves the measurement of psychological phenomena, through methods such as psychological testing, personality testing and intelligence testing.

[36] Cf *Crimes Act 1914* (Cth) ss 3ZH–3ZI.

[37] For example, the *Crimes (Amendment) Act 1997* (Vic) vastly expanded the category of people who could be ordered to provide body samples upon conviction of a crime to be entered into a DNA database.

there is no power to force such an examination to take place benefits will be suspended if there is an unreasonable failure to comply.[38] Such powers create the potential for abuse and can pose a threat to bodily privacy. As the Victorian Parliamentary Law Reform Committee is currently examining the limits on the powers of these bodies, however, the Commission does not intend to focus on this area.[39]

Genetic privacy

2.18 Many people are becoming increasingly concerned about their genetic privacy. People and agencies with an interest in genetic testing include the police, doctors, researchers, employers and insurance companies. The analysis of DNA can provide very sensitive health information. Determining how to balance a perceived need on the part of some agencies to procure such information, against the privacy concerns of the individuals tested, is critical. It is for this reason that a joint reference specifically relating to genetic privacy issues has been given to the Australian Law Reform Commission and the Australian Health Ethics Committee.[40] To avoid duplication of this work the Victorian Law Reform Commission does not intend to examine genetic privacy.

Biometrics and psychometrics

2.19 Biometrics and psychometrics provide another example of technological change which creates new challenges for the protection of bodily privacy. It is not uncommon for a prison to require visitors to undergo a retinal scan before entry to the prison, or a workplace to require employees to undertake psychological tests prior to employment. While the collation of data and use of the results of these tests may be protected by laws regulating information privacy, people may not wish to undergo the tests in the first place.

2.20 While actions for assault or battery would be available if a person was physically forced to submit to such tests[41] it will usually be the case that, under the law, people are regarded as having consented to the tests and so will have no legal remedies. In many cases, however, this 'consent' will not be genuine – people may feel they have no choice but to comply with the testing. This will be a particular problem in the employment context where a refusal to undergo such testing would often be detrimental to their employment. It is also increasingly becoming an issue in public places, where biometric technologies such as face recognition systems are being used without people's awareness or express consent.[42] Given the increasing use of such technologies

---

38 *Accident Compensation Act 1985* (Vic) ss 65 and 67.

39 The Inquiry examines powers of search and seizure for a range of bodies excluding the police. See Victorian Parliamentary Law Reform Committee Website for terms of reference, available at <http://www.parliament.vic.gov.au/lawreform>.

40 See <http://www.alrc.gov.au>. This issue is currently being considered in the US as well. On 23 June 2001, in his radio address to the nation, President Bush called on Congress to pass legislation to prevent genetic discrimination: <http://www.whitehouse.gov/news/releases/2001/06/20010623.html>. A Clinton Administration Executive Order, EO 13145, currently prohibits the use of genetic information within the federal government in hiring and promotion decisions: <http://www.nara.gov/fedreg/eo2000.html#13145>.

41 It should be noted that such actions may not be available in the case of psychometric testing as there is no physical contact involved.

42 This issue is discussed in further detail in Chapter 6.

and the issues raised by their use, this could be an appropriate area for the Commission to focus upon.

CONCLUSION

2.21 This Chapter has identified a number of areas where law reform may be necessary to protect bodily privacy. Issues which have been identified include:

- whether further safeguards are necessary to regulate the powers of police or other investigatory authorities to intrude on a person's body;
- whether genetic privacy requires legislative protection; and
- whether law reform is necessary to deal with biometric and psychological testing.

2.22 For reasons discussed above, the Commission does not believe that it would be timely to focus research into law reform on the areas of investigative powers or genetic privacy. However, the Commission believes that the issue of biometric and psychometric testing could be regarded as a priority area for law reform. This issue could be included as part of a broader examination of privacy in the workplace or, alternatively, in relation to surveillance in public places.

Chapter 3
Privacy and Physical Space

> *Claims to privacy advanced in a territorial or spatial sense are related historically, legally and conceptually to property. There is a physical domain within which a claim to be left in solitude and tranquillity is advance and is recognised*'.[43]

BACKGROUND

3.1 The concept of 'personal space' is fundamental to privacy. The violation of a person's personal or physical space may involve unauthorised entry into their home or business premises, or interference with their belongings. Such interference involves an incursion into a person's sense of personal safety and dignity as well as their property rights.

3.2 Historically, invasions of physical space mainly took the form of physical entry into people's homes, business premises or other premises, or tampering with their goods. Today, protection of privacy in physical space raises much broader issues. As the Australian Law Reform Commission commented some years ago, '[i]t is no longer possible to keep things private by locking the door, pulling the shades, [or] erecting a fence'.[44]

3.3 Intrusions into 'physical space' can now involve a number of different activities. These include the use of telephones and faxes (for example through unsolicited tele-marketing), the photographing of activities in private places or in public areas where people believe they are anonymous or unobserved, and the use of surveillance technologies including listening devices, concealed cameras and various types of sensors, which make it possible to discover what is happening in homes and business premises without entering them. The issue of surveillance in homes, workplaces and in public places is discussed in more detail in Chapter 6.

3.4 Some would argue that invasions of privacy in the electronic environment of cyberspace (for example, through surveillance of email and Internet browsing activity) should also be seen as invasions of 'personal space'. Given that most of these invasions either involve the interception or surveillance of communications, or an interference with personal 'information', rather than specifically focusing on 'cyberspace' as a separate area, we discuss these invasions within those particular contexts.[45]

---

[43] Department of Communications and Department of Justice, Canada, *Privacy and Computers* (1979) quoted in Australian Law Reform Commission, above n 6, para 47.

[44] Ibid, para 37.

[45] See Chapters 4 - 6.

HOW IS PRIVACY IN PHYSICAL SPACE PROTECTED?

Common law remedies against invasion of land

3.5 As in the case of bodily privacy, criminal law and civil remedies provide some protection for privacy in physical space. However, such remedies are primarily designed to protect property rights rather than privacy.

3.6 In the case of land, the common law differentiates between privately owned land and public space. The common law does not protect people from having their activities or movements scrutinised in public places, even in areas where they have the expectation that they will not be observed, for example, in public toilets.

3.7 Trespass and nuisance are the primary civil law remedies for invasions into or interferences with a person's home, business premises or other land. In certain situations, entry onto a person's land without their permission may also be a criminal offence.[46]

TRESPASS

3.8 If land is entered without authorisation, the person in possession can obtain monetary damages for past trespasses or an injunction to prevent further trespasses.[47] Trespass therefore operates indirectly to protect a person's privacy against intrusions by journalists, private investigators[48] and law enforcement agents who enter land and conduct searches without lawful authorisation.[49] A landowner can also protect their privacy by telling a person who has entered with permission to leave the premises, after which they will become a trespasser and can be evicted. However, by the time that permission is withdrawn, the person on the property may have already obtained access to private information which they may later seek to use or publish.

3.9 It is important to note that the purpose of the legal notion of trespass is to protect private property rights rather than to protect an individual's privacy. Therefore, it does not provide a remedy against privacy-invasive activities by an individual who is authorised to be on the premises.

---

[46] See below n 54.

[47] The principle was famously expressed by Lord Coke in the maxim that 'the house of everyone is to him as his castle and fortress': *Semayne's Case* (1604) 5 Co Rep 91a; 71 ER 194.

[48] See, eg, *Greig v Greig* [1966] VR 376, where a private investigator broke into a flat and installed surveillance equipment.

[49] If the person enters the property without permission they will clearly be a trespasser. In some cases, however, a right to enter may be implied. The extent of that implied right to enter will depend on the circumstances. For example, it will not be a trespass for a genuine client to enter a lobby of a business open to the public. It may, however, be a trespass for a journalist to enter that same space for the purpose of filming without authority: see *Lincoln Hunt (Aust) P/L v Willesee* (1986) NSWLR 457.

3.10 In some situations individuals or agencies who enter land without permission will not be liable for trespass. For example, the common law gives police a limited right to enter privately owned land for the purpose of arresting a person and searching the premises.[50] Common law powers to enter and search premises have been codified and extended by State[51] and Commonwealth legislation.[52] For example, State legislation permits Victorian police, without a warrant, to enter and search premises to arrest a person who has escaped legal custody, who is committing a serious offence, or is believed to have committed such an offence.[53] Police may also obtain a warrant from a magistrate permitting them to search buildings and places or to seize items which will provide evidence about the commission of serious offences.[54]

3.11 Powers to enter premises are also conferred on many other officials including council officers,[55] inspectors under the *Accident Compensation Act*[56] and fisheries inspectors.[57] As indicated in Chapter 2, these powers of entry and search by officials other than police were recently referred to the Victorian Parliamentary Law Reform Committee for review.[58] For this reason the Commission does not propose to focus on the extent of these powers.

NUISANCE

3.12 The legal action of 'private nuisance' may also provide some limited and indirect protection of privacy.[59] However, in *Victoria Park Racing and Recreation Grounds Ltd v Taylor*[60] the High Court of Australia refused to prevent a radio station from broadcasting a description of races from a tower which it had built on property next door to a racecourse. The case is often said to establish that the law of nuisance does not give occupiers of land any right of privacy, although Victoria Park's main concern in the case was to prevent loss of profits rather than

---

50 *Semayne's Case* (1604) 5 Co Rep 91a; 71 ER 194; *Leigh v Cole* (1853) 6 Cox CC 329; *Dillon v O'Brien* (1887) 16 Cox CC; *Plenty v Dillon* (1991) 171 CLR 635.

51 See, eg, *Crimes Act 1958* (Vic) s 459A. There are also other Victorian Acts authorising entry and search in specific situations: see below.

52 *Crimes Act 1914* (Cth) Part 1AA, VIA. There are numerous legislative provisions giving the Australian Federal Police, customs officers and other public officials powers to enter and search premises.

53 *Crimes Act 1958* (Vic) s 459A.

54 *Crimes Act 1958* (Vic) s 465. See also ss 466-470.

55 *Health Act 1958* (Vic) s 47C.

56 *Accident Compensation Act 1985* (Vic) ss 240, 240A, 248B.

57 *Fisheries Act 1995* (Vic) s 103.

58 See <http://www.parliament.vic.gov.au/lawreform>.

59 'Private nuisance' arises where there has been an unlawful interference with a person's use or enjoyment of land, or of some right over it, or in connection with it: *Hargrave v Goldman* (1963) 110 CLR 40.

60 (1937) 58 CLR 479.

interference with their privacy.[61] By contrast, more recent cases suggest that nuisance may provide some protection to occupiers of land against persistent and harassing video surveillance.[62]

Statutory remedies against invasion of land

3.13 State and Commonwealth legislation also give some piecemeal protection against invasions of physical space including:

- criminal laws which make it an offence to forcibly enter premises;[63]
- consumer protection legislation which requires door to door salespeople to leave premises immediately on the request of the occupier;[64]
- State and/or Commonwealth laws which penalise people who make offensive or harassing phone calls;[65]
- domestic violence and stalking laws which enable individuals to seek court orders to prevent a person from entering or approaching a home or a workplace, loitering near premises or phoning, sending electronic messages or otherwise contacting a person;[66] and
- legislation which regulates the use of surveillance devices.[67]

3.14 In light of the increasing availability of devices which enable people to obtain access to premises without entering them, the *Surveillance Devices Act 1999* (Vic) provides important privacy protection for physical space by imposing criminal penalties on the unauthorised installation, use and maintenance of optical surveillance devices (including cameras), listening devices, personal

---

[61] See also *Baron Bernstein of Leigh v Skyviews and General Ltd* [1978] QB 478, where trespass was held not to apply to an aerial photographer who flew over property to take photographs, because the owner's rights to airspace above the property did not extend to cover intrusion by aircraft.

[62] In *Raciti v Hughes* (1995) 7 BPR 14, 837 an injunction was granted to a landowner to prevent their neighbour from using video surveillance equipment which was switched on and began to operate every time the landowner or his family used the back yard. It is unlikely that the action of nuisance provides protection against privacy invasions which do not involve harassing or persistent behaviour. For other examples of where nuisance may provide a remedy, see *Stoakes v Brydges* [1958] QWN 5; *Khorasandjian v Bush* [1993] *New Law Journal* 329.

[63] Eg, *Crimes Act 1914* (Cth); *Summary Offences Act 1966* (Vic).

[64] See, eg, *Fair Trading Act 1999* (Vic) s 76. See also *Private Agents Act 1966* (Vic), which makes it an offence to enter onto property without lawful authority (s 27) and empowers the court to refuse to grant licenses to private agents if they have been involved in 'harassing tactics' (s 12). In addition, under the *Trade Practices Act 1974* (Cth) s 51AE, the Regulations may prescribe industry codes and declare them to be mandatory or voluntary. Contravention of an applicable code is a breach of the Act (s 51AD). To date, no direct marketing code has been prescribed. There are, however, industry codes of practice covering direct marketing, but these only bind members of the relevant industry associations.

[65] See, eg, *Crimes Act 1914* (Cth) s 85S.

[66] *Crimes Act 1958* (Vic) section 21A.

[67] *Surveillance Devices Act 1999* (Vic). For a more detailed analysis of surveillance, see Chapter 6.

location-tracking devices and data surveillance devices.[68] Consent is generally required before a person is put under surveillance.[69] The adequacy of the protection provided by this Act is discussed in more detail in Chapter 6.

Common law remedies protecting personal property

3.15 Where a person's goods are interfered with by, for example, an unauthorised search, the person affected may be able to obtain a civil remedy through the action of trespass to goods or conversion.[70] As in the situation of trespass to land, the primary purpose of these actions is to protect property rights. However, they may also provide some redress for privacy intrusion. In some situations a person who interferes with goods will also be criminally liable for theft.[71]

IS PRIVACY IN PHYSICAL SPACE ADEQUATELY PROTECTED?

3.16 Over time, courts have extended existing common law remedies to deal with new forms of privacy interference.[72] However because common law remedies were primarily intended to protect property rights, it is unlikely that they will ever provide adequate remedies against breaches of privacy.

3.17 Commonwealth and State legislation has extended the privacy protection provided by the common law. However, protection of privacy in physical space remains relatively piecemeal. Questions relating to privacy protection in physical space include:

- Should there be greater protection for privacy in public places?
- Should there be more extensive privacy protection for information obtained as the result of invasions of property?
- Is law reform needed to give workers protection against invasions of physical privacy in the workplace?
- Is law reform needed to give people greater protection against privacy-invasive technology?

These questions are discussed below.

---

[68] *Surveillance Devices Act 1999* (Vic) ss 6-8. We note that these protections only apply to 'private' spaces – similar restrictions do not apply in relation to surveillance in public places: see below.

[69] One exception arises in relation to optical or audio surveillance of a conversation or activity, where a participant to that conversation or activity is allowed to conduct surveillance without consent. This is known as 'participant monitoring'.

[70] Trespass to goods involves the direct, intentional interference with a person's goods. There is no need to damage the goods – simply to interfere with them in some way. Conversion involves dealing with goods 'in a manner repugnant to the immediate right of possession of the person who has the property': *Penfolds Wines Pty Ltd v Elliott* (1946) 74 CLR 204 at 209 per Dixon J. See also *Triffit v Dare and Bowater Tuft Industries Pty Ltd*, Tasmania Supreme Court Judgement No. A109/1993.

[71] See *Crimes Act 1958* (Vic) s 74. It is necessary to show that the accused has a dishonest intention.

[72] As an example, a United States judge has recently extended the law of trespass to prevent an internet company from using a software 'spider' to 'crawl' through another company's web site to extract information: see New York Times Cyberlaw Journal, 26 May 2001 <http://www.nytimes.com/library/tech/00/05/cyber/cyberlaw/26law.html>.

Privacy in public places

3.18 In the past, people in urbanised areas could rely on anonymity to protect their privacy when they were moving about in public. This anonymity has been eroded by technological developments and an increase in the use of surveillance technologies. For example, facial recognition technology has recently been used at some sporting events, allowing photographs or video footage of individuals entering the ground to be matched against other databases, so that the entrant can be recognised. Other examples include situations where:

- people are videoed or photographed[73] in public places including shops, hospitals, schools, childcare centres and on the street;[74]
- employees are subjected to various forms of surveillance by their employer, both within and outside the workplace;[75] and
- property is photographed from the street and published for news or advertising purposes.[76]

3.19 Often this surveillance will be covert, so people will not be aware that they are being observed. Even when surveillance of this type is overt, people often cannot avoid exposure without limiting their ability to go into particular public places.

3.20 Current laws do not protect privacy in public places even in areas where people have the expectation that they will not be observed. Laws relating to surveillance are limited to the 'private' domain. Given the rise in the use of such technologies, it is arguable that the current legal system does not give people adequate protection against having their activities or movements scrutinised in public places.

Information obtained as the result of invasion of physical space

3.21 Common law remedies which prevent intrusion into, or interference with private property may not prevent the publication of information which has been obtained as a result of the wrongful act. For example, the Supreme Court of New South Wales allowed a film made on Scientology premises, which the plaintiffs argued had been obtained as the result of a trespass, to be shown[77] However, in other cases injunctions have been granted to prevent the screening of such films.[78] In this area questions arise about the balance which should be struck between the

---

[73] For discussion of privacy relating to photographs see S Theedar 'Privacy in Photographic Images' (1999) 6 *Privacy Law and Policy Reporter* 75, available at <http://www.austlii.edu.au/au/journals/PLPR/1999/59.html>.

[74] If a person commissions a photograph to be taken, and it is published without their consent, they may have a remedy in copyright law: see *Williams v Settle* [1960] 2 All ER 806. If the image is defamatory there may be a remedy in defamation: see *Kirk v AH and AW Reed* [1960] NZLR 801. If a person's image is appropriated for commercial purposes they may have a remedy in passing off, or under the *Trade Practices Act 1974* (Cth) s 52.

[75] Although it may be argued that a workplace is a 'private' space (given its ownership by the employer), as most areas of the workplace fall outside the scope of the 'private' areas protected by the *Surveillance Devices Act 1999* (Vic), we treat it as a public place.

[76] *Bathurst City Council v Saban* (1985) 2 NSWLR 704.

[77] *Church of Scientology Inc v Transmedia Productions Pty* Ltd (1987) Aust Torts Reports 80-101.

[78] In *Emcorp Pty Ltd v ABC* [1988] 2 Qd R 169 the ABC was prevented from screening a film made by ABC employees who had trespassed on business premises.

privacy rights of individuals and the public interest in access to news and in the free flow of information. As similar problems arise in the area of surveillance, we discuss this problem again in Chapter 6.

Workplace privacy

3.22 Employers are increasingly using various technologies to monitor employee's activities, either on the employer's premises or elsewhere, including in employee's own homes while they are doing work for an employer. For example, workers may have their movements tracked through the use of location devices or biometric devices such as facial and voice recognition technology, or their activities may be monitored through various forms of surveillance. In many cases, employees are aware of surveillance and are seen as having 'consented' to it. Such consent may be required as a condition of employment or be inferred from the fact of employment.[79] People in these circumstances may feel they have no meaningful ability to refuse consent and/or they may not be aware that they can do so.[80]

CONCLUSION

3.23 This Chapter has identified a number of areas where law reform may be necessary to protect physical privacy. Current legislative provisions are piecemeal and do not fill the gaps left by the common law. It is clear that major gaps in privacy protection include:

- lack of legal protection for privacy invasions in public places; and
- lack of protection for employees against invasions of physical privacy.

3.24 The Commission's initial research and consultation indicates that the increasing use of surveillance in both public places and workplaces is a matter of considerable community concern. This suggests that these may be priority areas for a review of the law relating to privacy.

3.25 If the Commission focuses its research on the issue of surveillance in the workplace, it would be necessary to determine whether this should be part of a broader project on privacy in the workplace. As will be seen in Chapter 7, some aspects of workplace privacy involve issues of Commonwealth law which it may be inappropriate for the Commission to investigate. We return to a more detailed examination of the proliferation of surveillance technologies and their impact on privacy in Chapter 6.

---

[79] 'Implied consent' is frequently used as a defence against apparent breaches of surveillance laws: see J Sempill, 'Under the Lens: Electronic Workplace Surveillance', forthcoming *Australia Journal of Labour Law*.

[80] For a more detailed consideration of workplace privacy issues, see Chapter 7.

Chapter 4
Information Privacy

There really are ghosts – every one of us is followed around by an invisible profile that purports to be who we are.[81]

BACKGROUND

4.1 Expressions such as the 'information age', the 'information revolution', the 'information explosion' and the 'information society' all attempt to capture the magnitude of the change being experienced as a result of the extraordinary growth of information technologies. Vast trails of data about people are generated during their everyday activities. The widespread adoption of the Internet is making people far more conscious of, and concerned about, privacy of information.

4.2 There are many reasons why individuals disclose information about themselves and allow organisations to keep personal information about them. Sometimes it is because they are required to or because the provision of a particular product or service is conditional upon them giving that information, such as when they are applying for a credit card or a government benefit. Other times it is because they are providing it for a particular purpose, such as when they enter a competition or make a charitable donation. When people provide information in one context, they often do not realise that this information may ultimately be used for other purposes as well.

4.3 The increasing collection of personal information affects privacy in many ways. Information can be collected or passed on to others without the individual knowing anything about it, such as when they are tracked by cookies[82] over the Internet or their raffle ticket contact details are sold to direct marketers. Information from different sources can be combined together to develop surprisingly detailed profiles on individuals. It might not be kept securely or it might be recorded inaccurately. These are all issues which privacy laws seek to address.

4.4 In this Chapter we examine how information privacy is protected in Australia. We begin by examining the Commonwealth and Victorian Privacy Acts and the information privacy principles contained within them. We then look at the exemptions to those Acts before focusing on the gaps in the scheme and possible areas for reform.

---

[81] Don Goldhammer, University of Chicago, quoted in John Schwartz and Robert O'Harrow Jr, 'Databases start to fuel consumer ire', (10 March 1998) *Washington Post,* available at <http://www.washingtonpost.com/wp-srv/frompost/march98/privacy10.htm>.

[82] See the Glossary at the end of this Paper for a definition of 'cookies'.

HOW IS INFORMATION PRIVACY PROTECTED?

4.5 Historically, the common law has provided little privacy protection for personal information.[83] As threats to privacy have been heightened by the rapid growth of new information and communication technologies, legislation has been enacted to give individuals some degree of control over *who* knows *what* about them and *why*. To date, providing for some level of information privacy has been the main focus of legislative privacy protection in Australia.

4.6 There is no legislation which provides general privacy protection for all personal information. Commonwealth and State legislation provides privacy protection in specific situations but also places some limits on this protection. Some of the factors which determine what kinds of privacy rights are protected by legislation are:

- whether the information is held by a public or private sector organisation. In the past, personal information held by the public sector had more extensive privacy protection than personal information held in the private sector. Commonwealth privacy legislation has now been extended to cover the private sector (with some major exemptions) but there are still substantial differences in the coverage of the public and private sector;

- the type of information and the person to whom it is disclosed – for example, there are restrictions on the disclosure of patient's personal information by doctors[84] and specific laws govern the handling of health records in Victoria;[85]

- whether the information is held on a public register. Limited privacy rights are created by legislation establishing public registers, such as the Electoral Roll, and the Births, Deaths and Marriages Register;[86]and

- the nature of the industry which holds the information – for example, specific privacy provisions apply to businesses in the telecommunications industry[87] and between banks and their customers.[88]

In addition, legislation may protect privacy by penalising unauthorised access to information, for example by computer hacking.[89]

---

[83] If information is communicated confidentially, the person whose information was disclosed might have a remedy for breach of confidence. See, eg, *Commonwealth of Australia v. John Fairfax and Sons Ltd* (1980) 147 CLR 39; *Smith, Kline and French Laboratories v. Department of Community Services and Health* (1991) 99 ALR 679.

[84] See, eg, provisions in health legislation such as *Health Services Act 1988* (Vic) s 141 and *Mental Health Act 1986* (Vic)

s 120A. The common law may also provide remedies against doctors for disclosure of confidential information.

[85] Victorian health service providers (in the public and private sector) will have to comply with the Health Privacy Principles set out in the *Health Records Act 2001* (Vic) once it comes into force on 1 July 2002.

[86] See *The Constitution Act Amendment Act 1958* (Vic) s 66; *Commonwealth Electoral Act 1918* (Cth) s 104; and *Births, Deaths and Marriages Registration Act 1996* (Vic) s 44.

[87] See Part 13 of the *Telecommunications Act 1997* (Cth) and the complementary Industry Code adopted by the Australian Communications Industry Forum (ACIF) on the 'Protection of Personal Information of Customers of Telecommunications Providers', December 1999.

[88] In addition to the common law duty of confidence, credit providers are required to comply with Part IIIA of the *Privacy Act 1988* (Cth).

Privacy rights under general privacy legislation

4.7 Privacy legislation in Australia has been influenced by the privacy guidelines developed more than two decades ago by a committee of the Organisation for Economic Cooperation and Development (OECD), under the chairmanship of Justice Michael Kirby.[90] The OECD Guidelines incorporate eight principles relating to the collection, purpose, use, quality, security and accountability of organisations in relation to personal information. However, the OECD Guidelines do not set out requirements as to how these principles are to be enforced by member nations. As a result, OECD member countries have chosen a range of differing measures to implement the privacy principles. Australia officially adopted the OECD Guidelines in 1984.

4.8 Commonwealth and State privacy laws seek to protect the individual's right to privacy by providing rights applicable throughout the lifecycle of information held by organisations from the time of its collection to its ultimate destruction. The legislation seeks to balance these rights against other public interests such as law enforcement and the efficiency of public administration.

4.9 The *Privacy Act 1988* (Cth), covering Commonwealth Government agencies, commenced in 1989. This Act was recently extended by the *Privacy Amendment (Private Sector) Act 2000* (Cth) to cover private sector organisations and begins operation in December 2001.[91] In Victoria, the *Information Privacy Act 2000* was recently passed and comes into force in September 2001. It covers State Government agencies and private contractors to State Government.[92] Similar public sector privacy legislation was also passed in New South Wales in 1998[93] and is being considered in other jurisdictions.[94] Most industrialised countries have passed similar laws in recent decades.[95]

4.10 The manner in which the Commonwealth and Victoria have chosen to implement privacy protections is by setting out 'information privacy principles' that provide general privacy protection for personal information, subject to some important exceptions.

---

[89] Unauthorised access to computer systems is prohibited in Victoria: *Summary Offences Act 1966* (Vic) s 9A. Interferences with mail, telecommunications and data stored on Commonwealth computers are also prohibited: *Crimes Act 1914* (Cth) Parts VIA, VIIA and VIIB.

[90] OECD, *Guidelines for the Protection of Privacy and Transborder Flows of Personal Data*, adopted 23 September 1980, available at <http://www.oecd.org/dsti/sti/it/secut/prod/PRIV-en.HTM>.

[91] Although the provisions of this Act do not come into force until 21 December 2001, throughout this Paper we refer to the amendments made by this Act as if they were already operational. References to the *Privacy Act 1988* (Cth) therefore include the as yet non-operational amendments made by this Act.

[92] This legislation expressly excludes health records from its coverage, as the intention was to enact complementary legislation protecting health information. The *Health Records Act 2001* (Vic), which will come into force in July 2002, covers both public and private health service providers, and gives patients a right of access to their health records held by private practitioners.

[93] *Privacy and Personal Information Protection Act 1998* (NSW).

[94] For example, the Northern Territory intends to introduce public sector privacy legislation to complement the Commonwealth regime: Ministerial Statement of the Chief Minister of the Northern Territory, the Hon. Denis Burke MLA, *Northern Territory Hansard*, 22 April 1999, available at <http://notes.nt.gov.au/lant/hansard/HANSARD8.NSF?OpenDatabase>.

[95] For a comprehensive survey of the coverage of privacy and data protection laws around the world, see the Privacy International website <http://www.privacyinternational.org/survey/index.html>.

INFORMATION PRIVACY PRINCIPLES

4.11 The information privacy principles incorporated in the Commonwealth *Privacy Act 1988*[96] and the Victorian *Information Privacy Act 2000* deal with the following matters:[97]

- **Collection of personal information:** Collection must be necessary for the activities of those who collect the information, it must be collected lawfully and fairly, and at the time it is collected individuals must be told who is collecting the information and how it will be used.

- **Use and disclosure of personal information:** As a general principle, information can only be used or disclosed for its original purpose unless the person has consented to its use or disclosure for another purpose.

- **Accuracy of personal information:** Reasonable steps must be taken to ensure that personal information is accurate, complete and up-to-date.

- **Security of personal information:** Reasonable steps must be taken to protect the personal information from misuse, loss, unauthorised access, modification or disclosure.

- **Openness in relation to the practices:** Those who collect personal information must set out in a document their practices and must make this document available.

- **Access and correction rights:** As a general principle, individuals must be given access to their personal information and must be allowed to correct it or attach to it a statement claiming that the information is not accurate, complete or up-to-date.

- **Use of unique identifiers:** Organisations cannot use an identification number uniquely assigned by another organisation, such as a government agency, as their own identifier. This is intended to prevent the development of a national identity number.

- **Anonymity:** Private sector organisations and Victorian public sector agencies must give people the option of entering into transactions anonymously where it is lawful and practicable.[98]

- **Restrictions on transborder data flows:** As a general principle, private sector and Victorian public sector organisations[99] can only transfer personal information about an individual to a foreign jurisdiction (i.e. outside Australia or Victoria) if they believe that

---

96 Under the *Privacy Act 1988* (Cth), the privacy principles that apply to the public sector are known as 'Information Privacy Principles', and the principles that apply to the private sector are known as 'National Privacy Principles'.

97 It should be noted that these principles will not apply to all bodies that hold personal information. As noted above, there are slightly different requirements for public and private sector bodies. In addition, there are a number of exemptions to the scheme (outlined below).

98 The anonymity principle is not reflected in the Commonwealth public sector Information Privacy Principles.

99 The transborder data flow principle is not contained in the Commonwealth public sector Information Privacy Principles.

the information will be protected by a law or a contract which upholds privacy principles similar to the information privacy principles, or if the individual gives consent.

- **Special provisions for sensitive personal information:** A higher level of privacy protection applies to sensitive personal information which includes information about a person's health, political or religious beliefs or affiliation, and sexual preference. The private sector and Victorian public sector information privacy principles require that this information must only be collected with the individual's consent.[100]

4.12 If an organisation breaches any of these privacy principles the person whose privacy is affected should first complain to that organisation. If the organisation fails to deal with the complaint adequately the affected person can then lodge their complaint with the Commonwealth or State Privacy Commissioner.[101] Where the relevant Privacy Commissioner believes that the privacy law has been breached, the organisation may be required to take some appropriate action. This action could involve an apology, a change in procedures, the correction or deletion of personal information, or payment of compensation for the harm suffered.

Balancing privacy protection against other policy goals

4.13 The Victorian and Commonwealth privacy laws contain a number of exemptions. To some extent these recognise the balance between an individual's right to have their personal information kept private, and the public interest which may be served in having access to such information for purposes such as the apprehension of criminals and the protection of national security. The exemptions also reflect political compromises which were considered necessary to ensure the passage of the legislation. Exemptions apply in the following areas:

- **Courts and the administration of justice:** State and Commonwealth public sector privacy laws have a limited application to courts and tribunals. Neither the Victorian *Information Privacy Act 2000* or the Commonwealth *Privacy Act 1988* apply to courts and tribunals when handling personal information to fulfil their judicial and quasi-judicial functions (although the Act would still apply to personal information collected for other functions, for example the maintenance of staff records).[102] This limitation on the protection of individual privacy reflects the view that the open administration of justice is in the public interest. It has nevertheless been recognised that there can be a tension between privacy interests and the administration of a fair and open justice system. For example, while courts are generally open to the public, the identification of parties in matrimonial and certain criminal proceedings is restricted.[103]

---

[100] The Commonwealth public sector is only bound by privacy principles in relation to certain kinds of sensitive information. For example, a person's criminal history cannot be disclosed where the convictions were spent, quashed or pardoned: *Crimes Act 1914* (Cth) Part VIIC.

[101] Paul Chadwick has recently been appointed as the first Victorian Privacy Commissioner.

[102] *Information Privacy Act 2000* (Vic) s 10; *Privacy Act 1988* (Cth) ss 6(5)(d) and 7(1)(a)(ii).

[103] See, eg, *Family Law Act 1975* (Cth) s 121, which prohibits the publication, by electronic or any other means, of an account of court proceedings that identifies a party or witness (including their title, alias or pseudonyms; their physical description or style of dress; their occupation or work address; and their recreational interests, religious or political beliefs).

- **Law enforcement and national security:** In both the Victorian and Commonwealth Acts, specified law enforcement and intelligence agencies are exempt from having to comply with certain privacy principles.[104]

- **Political representatives and conduct of elections:** Members of Parliament are generally exempt from privacy laws. Under the Victorian legislation only Ministers and Parliamentary Secretaries have to comply with the privacy principles. Other Members of Parliament are not required to comply with the Act.[105] The Commonwealth legislation also provides a wide exemption for registered political parties and the acts of political representatives when engaged in an election or another part of the political process.[106] The reason for this exemption has been expressed as being for the preservation of the freedom of political communication.[107]

- **Free speech and free press:** The Commonwealth private sector privacy legislation exempts media organisations engaged in journalism provided they are publicly committed to observing a set of standards that deal with privacy.[108] This is intended to balance the privacy rights of individuals with the public interest in a free flow of information. The exemption leaves responsibility for solving privacy issues to individual media organisations. The adequacy of the media's complaints handling schemes and standards was recently questioned by the Senate Select Committee on Information Technologies.[109]

- **Libraries and archives promoting study and reference:** Neither the Commonwealth nor the Victorian privacy laws apply to personal information held in government records archives[110] or reference collections (such as those kept in libraries and museums).[111] The library exemption promotes the free flow of information and avoids the application of privacy principles which would require libraries to ensure that the personal information contained in their collections is up-to-date and accurate, or to restrict access to the information.

---

[104] *Information Privacy Act 2000* (Vic)s 13; *Privacy Act 1988* (Cth) ss 7(1)(a)(iv), 7(1)(f)-(h), 7(1A) and 7(2). Under the Commonwealth Act, the Australian Federal Police are bound by many of the information privacy principles, although there are certain exceptions contained within the principles.

[105] *Information Privacy Act 2000* (Vic) s 9. Despite being exempt from the Victorian legislation, Members of Parliament will be subject to a voluntary privacy code, in recognition that 'it would not be acceptable to leave MPs entirely outside a privacy protection framework': Victoria, Parliament, Scrutiny of Acts and Regulations Committee, *Report on an Interim Code of Conduct for Members of the Victorian Parliament*, May 2001, available at <http://www.parliament.vic.gov.au/sarc/InfoPriv/tocinterim.htm>.

[106] *Privacy Act 1988* (Cth) ss 6C(1) and 7C.

[107] Australia, Attorney-General, the Hon. Daryl Williams AM QC MP, *Exemption for bodies registered under electoral laws and political representatives*, fact sheet, 22 December 2000, available at <http://www.ag.gov.au/privacy/newfacts/PoliticalParties.html>.

[108] *Privacy Act 1988* (Cth) s 7B(4).

[109] *In the Public Interest: Monitoring Australia's Media*, available at <http://www.aph.gov.au/senate/committee/it_ctte/selfreg/index.htm>. In April 2000, the Committee recommended the establishment of an independent statutory body (the Media Complaints Commission) to handle more serious privacy complaints.

[110] Archived materials generally only become available to the public after considerable time has passed: see, eg, *Public Records Act 1973* (Vic) s 10, which allows for records to be withheld for 30 years.

[111] *Information Privacy Act 2000* (Vic) s 11. See also *Privacy Act 1988* (Cth) s 6, which excludes information held in places such as libraries, museums or Commonwealth archives from the definition of 'records'.

- **Generally available publications (including public registers):** The Commonwealth and Victorian public sector privacy laws have a restricted application when it comes to 'generally available publications' (such as newspapers, books, annual reports or public registers). Under the Commonwealth legislation, the collection principle (requiring lawful and fair collection) and the openness principle (requiring documentation of organisational principles) applies to information that is to be included in such publications but the security, access, use and disclosure principles do not.[112] The Victorian legislation takes a different approach. None of the privacy principles under the Act apply to generally available publications.[113] However, in the case of public registers[114] the legislation obliges those administering the public registers to comply with the privacy principles 'so far as is reasonably practicable'.[115] The intention of this provision is to ensure that information is collected and used only for the legitimate purposes for which the public register was established. Bodies responsible for compiling public registers cannot use the information for other unrelated purposes, such as direct marketing.[116]

- **Direct marketing:** The Commonwealth private sector principles allow private sector organisations to use personal information for the purpose of direct marketing without first obtaining an individual's consent, if it is impracticable to obtain that consent and if the organisation provides the individual with an opportunity to opt out of receiving further communications.[117] To require prior consent in all cases was seen by the Commonwealth Government as having a significant negative impact on an industry which is essentially based around the trade of information.[118]

- **Small business:** As the Victorian *Information Privacy Act 2000* applies only to the public sector, small businesses will not fall within its scope.[119] Although the Commonwealth *Privacy Act 1988* has recently been extended to cover the private sector, it provides an exemption for small businesses.[120] Under the Act, small businesses are defined as businesses with an annual turnover of $3 million or less, but not including those businesses which handle health information, trade in personal information, are part of a larger business group, or who opt into the privacy scheme.[121] The Commonwealth Government, when introducing the legislation into Parliament, justified this exemption

---

112 The definition of 'record' in *Privacy Act 1988* (Cth) s 6 excludes generally available publications. See also the Information Privacy Principles and National Privacy Principles.

113 *Information Privacy Act 2000* (Vic) s 11.

114 Public registers are lists that are usually required to be made available to the public under statute or regulation: see *Information Privacy Act 2000* (Vic) s 3.

115 *Information Privacy Act 2000* (Vic) s 16(4).

116 Explanatory Memorandum to the *Information Privacy Bill 2000* (Vic), note to cl 11.

117 *Privacy Act 1988* (Cth) National Privacy Principle 2.1(c).

118 Explanatory Memorandum to the *Privacy Amendment (Private Sector) Bill 2000* (Cth), p 29.

119 The *Health Records Act 2001* (Vic) applies to health records held either in the public or private sector, and so will apply to small businesses.

120 *Privacy Act 1988* (Cth) s 6C.

121 *Privacy Act 1988* (Cth) ss 6D-6EA.

on the basis that it was necessary to avoid unreasonable or excessive compliance costs being imposed on businesses who were considered to be a low privacy risk.[122]

- **Employee records held by private sector organisations:** Public sector employee records must be handled in accordance with the privacy principles under the State and Commonwealth privacy legislation. Employee records in the private sector are not similarly protected. Private sector organisations do not have to comply with the Commonwealth privacy law when handling employee records in the context of a current or former employment relationship.[123] The Commonwealth Government took the view that employee privacy was better dealt with under workplace relations legislation[124] which it has pledged to review in consultation with the States and Territories.[125]

IS INFORMATION PRIVACY ADEQUATELY PROTECTED?

4.14 Despite significant developments in the legal protections offered for information privacy in Australia, substantial gaps still exist. In particular, exemptions for employee records and small businesses under the Commonwealth *Privacy Act 1988* make it difficult to build consumer confidence in electronic commerce, given widespread consumer privacy concerns.[126] The problem of these exemptions was highlighted in the recent assessment of the *Privacy Act 1988* by the European Commission's data protection working party which indicated that it did not meet European standards of adequacy for data protection.[127] Although the European Union has not yet made an official decision about the adequacy of Australia's data protection scheme, a finding of inadequacy would result in extra-legal measures (such as the use of contractual privacy provisions) being required in order to safeguard personal information that was transferred from European countries into Australia.[128]

4.15 Although many have been critical of the new Commonwealth and State information privacy legislation, the Commission does not believe that it is appropriate to review the State legislation so soon after its passage. There is already a commitment by both governments to review the legislation after two years of operation. This would allow the relevant agencies to proceed with implementation without being unduly hampered by revisiting issues which have already been subjected to widespread debate. Complaints made to the Commonwealth or

---

122 Explanatory Memorandum to the *Privacy Amendment (Private Sector) Bill 2000* (Cth), p 36.

123 *Privacy Act 1988* (Cth) s 7B(3). As State laws only apply to the public sector, private sector organisations do not have to comply with the State privacy principles in relation to employee records.

124 Explanatory Memorandum to the *Privacy Amendment (Private Sector) Bill 2000* (Cth), pp 80-81.

125 Australia, Attorney-General, the Hon. Daryl Williams AM QC MP, *Employee records*, fact sheet, 22 December 2000, available at <http://www.ag.gov.au/privacy/newfacts/EmployeeRecords.htm>.

126 See, eg, Roy Morgan Research Centre Inc, '"Big Brother" Bothers Most Australians' (30 August 1999) *The Bulletin*, available at <http://www.roymorgan.com/polls/1999/3221/>.

127 Working Party on the Protection of Individuals with Regard to the Processing of Personal Data set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, *Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000*, adopted on 26th January 2001, available online at the European Commission's website at <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp40en.htm>.

128 See Article 25 of the European Union's data protection directive and associated national laws.

Victorian Privacy Commissioner will allow the identification of problems and gaps in the legislation over the next few years.

4.16 There are, however, two areas of information privacy which might be considered appropriate subjects for law reform. These are:

- employee records; and
- public registers.

These are discussed in more detail below.

Employee records

4.17 If the Commission were given a reference on workplace privacy, employee records could be considered as part of this reference. It would, however, be necessary to carefully consider the interaction between State and Commonwealth schemes in this area.

Public registers and publicly available information

4.18 Public records[129] and publicly available information[130] are rich sources of personal information. Traditionally, due to the fragmented way in which publicly available records containing personal information have been stored and retrieved, it has only been possible to obtain this kind of personal information in relation to one person at a time, and obtaining it has generally involved visiting a particular place and waiting for a response to an individual request for the information. The practical and technological barriers to obtaining information on these registers has served as a de facto privacy safeguard for most people.[131]

4.19 These barriers are rapidly being broken down by the use of new technologies. The increasing 'computerisation' of such records now allows information from publicly available sources to be easily compiled, data-mined and cross-matched to form rich profiles of individuals. Private companies are increasingly able to compile profiles of individuals from these public registers which they can then cross-match with other public information (such as telephone books, newspaper archives and alumni directories) to come up with a rich storehouse of information. Profiling can be used to achieve beneficial ends, such as reducing fraud, protecting the public revenue and fighting crime. But it also creates significant risks to individuals particularly in the case of sensitive information (such as criminal history records) which may pose

---

129 'Public records' may include motor vehicle registrations, land titles, birth death and marriage registries, electoral rolls, business names registers, incorporation records, Australian Business Name (ABN) records, bankruptcy records, occupational and recreational licenses, criminal and court records.

130 'Publicly available information' may include newspapers (and classified advertisements), magazines, books, telephone books, email directories, school yearbooks, professional directories, genealogical databases, and may also include internet homepages and newsgroup postings.

131 Some public register legislation also includes special provisions allowing a person to apply to suppress their listing if its public availability endangers them or their family: see, eg, *The Constitution Act Amendment Act 1958* (Vic) s 66, which allows for removal of a person's address from the electoral roll on the grounds of personal safety.

threats to a person's safety and their ability to participate in society and access services and employment.[132]

4.20 These risks were highlighted last year when the Victorian Supreme Court aborted a murder trial after information about the accused was posted on the website of CrimeNet. This company provides the public with paid access to a database containing details of convictions and other general court information, compiled from publicly available Australian court records and newspapers.[133] Similar issues were highlighted when the *News of the World* newspaper in the United Kingdom conducted a 'name and shame' campaign against alleged paedophiles publishing names, pictures and locations of paedophiles. The campaign triggered a wave of vigilante attacks on men who were named as paedophiles, some of whom had been mistakenly identified.

4.21 The need to consider the protection of personal information contained in publicly available information is heightened by the fact that individuals often have no choice about whether this information is collected and made available.[134] As the information is usually provided for specific public purposes (such as to obtain a service or fulfil a legal obligation) people may not realise that it will be made public and could be used for commercial purposes. With increasing expectations for governments to deliver services and information (including public register information) online, the risk of misuse of personal information is amplified.

4.22 As noted above, current Victorian legislation provides limited privacy protection for personal information available from public sources. There are many practical reasons why public registers and other sources of public information, should not be expected to fully comply with the privacy principles contained in the privacy legislation. For example, if public access to names and addresses on electoral rolls was restricted there may be a greater risk of electoral fraud going undetected. However, without adequate safeguards to ensure that these databases and profiles of personal information are accurate and secure, accessible and correctable, and used for proper purposes, there is a risk of people being unfairly denied access to full participation in the community (including access to employment, rental accommodation or professional and club membership).[135] Ready access to personal profiles can also result in 'identity theft' where your personal information (name, driver's licence number, credit card details) is used by another person to commit fraud or other crimes,[136] as well as to incite vigilantism and discrimination on

---

132 For a discussion of the beneficial and harmful uses associated with personal information that is publicly available, see United States, Federal Trade Commission (December 1997) *Individual Reference Services: A Report to Congress*, available at <http://www.ftc.gov/bcp/privacy/wkshp97/index.html>. See also the Federal Trade Commissioner's *Identity Theft* website at <http://www.consumer.gov/idtheft/>.

133 The details about the accused's earlier conviction, which had been gathered from an article in the *Herald Sun* in 1988, were considered to have prejudiced his right to a fair trial.

134 For example, the Electoral Roll, land titles information, company incorporation and births, deaths and marriages are all mandatory public registers.

135 The release of potentially embarrassing personal information (such as library or video borrowing history) could also be used to dissuade someone from running for public office. See, eg, the introduction of the *Video Rental Privacy Protection Act 1988* in the United States, after a Washington D.C. newspaper publicised the video rentals borrowed by Judge Robert Bork, nominee for the Supreme Court: Dennis McDougal, 'Video Rental Privacy Bill Introduced', *Los Angeles Times*, 23 October 1987.

136 See 'identity theft' websites run by the United States Federal Trade Commission at <http://www.consumer.gov/idtheft/> and by Mari Frank, attorney and author of the *Identity Theft Survival Kit*, at <http://www.identitytheft.org/>, last visited 29 June 2001.

the basis of sensitive information.[137] In addition, if information is incomplete or incorrect, the purpose of the register may be undermined.

CONCLUSION

4.23 For the reasons discussed above, the Commission believes it should not undertake a general review of the adequacy of legislation protecting personal information held by the public or private sector. However, because State and Commonwealth privacy legislation provides only limited (and vague) protection for information held on public registers, we believe that this may be a priority area for investigation. The issue of employee records could also be considered if the Commission were given a general reference on workplace privacy.

Increasingly there is integration between information and communications technology. While information created by or facilitated by communication networks is covered by the recent privacy laws outlined in this Chapter, the process of communication of the information is not completely protected. The following Chapter examines the privacy protections that exist for private communications.

[137] See the above discussion of CrimeNet and *News of the World*'s 'name and shame' campaign.

Chapter 5
Communications Privacy

> *People who wish to communicate privately, by whatever means, are entitled to respect for privacy, even when communicating in otherwise public places.*[138]

> *It is said that the only privacy the sender of e-mail has depends upon the 'honesty, ignorance and indifference' of those operating computers over which the message passes.*[139]

BACKGROUND

5.1 The right to private communications is a crucial individual right. Personal communications can often involve intimate and sensitive information about individuals and their relationships. They may involve political commentary and criticism. They may also include socially sensitive matters including the fact that an individual is suffering or has suffered from depression, alcohol abuse or illness, or that an individual has a particular sexual orientation.

5.2 By ensuring the privacy of personal communications a society allows individuals to exchange ideas freely and to develop their ideas without the fear of either being misunderstood, having their comments taken out of context, or being penalised in some way. If individuals cannot communicate with some assurance of the privacy of their communications there is likely to be a chilling effect over time - making communications more stilted and preventing intimacy, the free exchange of ideas and free political expression.

5.3 There are a number of ways in which personal communications can be interfered with: they can be completely blocked, they can be monitored by a third party, they can be recorded by a participant to the communication without consent and then subsequently published, or records of the communications could be read or searched. Traditionally, those activities which involved the routine monitoring of communications have been classified as 'surveillance'. This has been contrasted with one-off interferences with communications, such as reading a particular piece of mail or with the actual blocking of the communication. In light of the increasing use of electronic forms of communications, however, this distinction no longer seems viable. Computer programs are now available which will automatically scan all email messages for a particular word, and then stop the intended recipient from receiving the communication if it contains that word, or send a copy of the communication to a third party. No-one is actually physically reading all of the communications in this case yet they are being monitored. Similarly, web-bugs have the capacity to track a person's movement around and communications on the Internet and to send that

---

[138] Australian Privacy Charter, Article 7.

[139] Kent Davey, above n 3.

information to a third party for marketing or other purposes. While this would not typically be considered 'surveillance' the person's actions are being surveilled even if it is in a limited sense.

5.4 While it would be possible to draw an artificial distinction between those forms of monitoring which are classified as 'surveillance' and those which do not fall within that category, for the sake of simplicity we have chosen to define 'surveillance' in its broadest possible sense: as the accessing or monitoring of a person's communications or activities in any manner whether it is a one-off or routine occurrence. We note that this definition of 'surveillance' is broader than simply monitoring communications. It would also include monitoring a person's activities whether they are at home or in a public place. Some forms of surveillance are regulated by state law. It is for these reasos that we discuss surveillance in the next Chapter[140] even though there is a substantial overlap with communications privacy.

5.5 In this Chapter we therefore give a brief overview of the law as it relates to communications privacy. We continue our discussion of communications privacy in the next Chapter, in the broader context of surveillance.

NEW CHALLENGES

5.6 Although recognition of the right to privacy in communications has a long history,[141] the development of a range of new technologies has created new problems. In particular, communications in an electronic environment create privacy protection problems which differ from those applicable to traditional one-to-one communications. At a practical level they involve a greater number of parties. At the sender's end there may be an employer who owns the computer network and an Internet Service Provider (ISP) who sends the message. At the receiver's end there may be an ISP that receives the message and a third party network owner. Between them there will likely be a telecommunications company that carries the message between the ISPs. The original communication may have been made to several parties at the same time, either because an email is sent to several recipients or because it occurs in a multi-party environment such as via a newsgroup or in a chat room.

5.7 Given the number of parties that the communication may have passed between, it is possible that it will have been permanently recorded in several places. This creates multiple opportunities for accessing the information contained within the communication. If the communication was made in an open chat room environment, the record of the communication may be permanently searchable through a search engine such as *Deja*.[142] This proliferation of

---

[140] See Chapter 6.

[141] Concerns about the interception of private mail were, for example, raised in a House of Commons report in June 1742 which revealed that an independent office within the Post Office operated purely for the purpose of intercepting letters: see Joyce, *History of the Post Office*, quoted in New Zealand Privacy Commissioner's Report to the Minister of Justice on the Postal Services Bill, 24 June 1997, available at <http://privacy.gov.nz/people/post.html>.

[142] This service was previously accessible at <http://www.deja.com> but has recently been acquired by Google.com and is now available at <http://groups.google.com/googlegroups/deja_announcement.html>.

possible ways to monitor communications creates a variety of new challenges for privacy protection.

LINKS BETWEEN INFORMATION AND COMMUNICATIONS PRIVACY

5.8 The extent to which the law recognises an individual's right to private communications is linked to the recognition of information privacy rights. This reflects the fact that information and communications technologies are now closely integrated - for example, most computers now come with pre-installed modems. Personal desktop, laptop and handheld computers, which were once primarily information devices, are increasingly integrated with communications technology; at the same time mobile phones, which were once communications devices, now store and access an increasing amount of information.

5.9 Any communication which occurs across networks and involves the exchange of data is likely to come within the scope of information privacy regimes such as the Commonwealth *Privacy Act 1988.*[143] Obligations would arise in relation to the collection, disclosure, retention and security of the personal information that is communicated.[144] For example, an e-mail communication between two government agencies containing personal information would be covered by the *Privacy Act* in relation to the record of the communication. However, the *Privacy Act* does not provide specific privacy safeguards relating to the *process* of *communicating* personal information (although obligations relating to maintaining data security are relevant to how the data is communicated) and it is necessary to look elsewhere to see how the law recognises privacy rights in communications.

HOW IS COMMUNICATIONS PRIVACY PROTECTED?

Common law

5.10 The common law provides some limited protection for private communications in situations where:

- the disclosure of personal communications would constitute a breach of confidence (such as communications between a doctor and patient);[145]
- a privileged relationship exists, such as between a solicitor and client, a doctor and patient, a priest and penitent and a reporter and their source;[146]
- the process of recording or listening involved some form of trespass, for example where a person has intruded on land to install a surveillance device;[147]

---

143 The basic test of whether the *Privacy Act 1988* applies is whether personal information exists in a record: s 16. This would not be the case if the information was contained in a communication which was not retained.

144 See Chapter 4.

145 See also *Evidence Act 1958* (Vic) ss 32B-32G.

146 See also, eg, *Evidence Act 1958* (Vic) ss 27-28; *Health Services Act 1988* (Vic) s 141.

- an action of nuisance is available to restrain the making of unwanted or threatening phone calls.[148]

Each of these protections are quite limited and although they offer some incidental privacy protection, they are generally concerned with issues other than privacy.

Legislation providing communications privacy protection

5.11 Some legislation also provides incidental privacy protection for communications. For example, copyright laws may protect private communications as a by-product of protecting a person's copyright in an original work.[149]

5.12 Over time, laws providing more specific privacy protection have developed in response to threats to communications privacy. Laws prohibiting unauthorised opening of mail[150] are an early example. Since that time, the Commonwealth *Telecommunications (Interception) Act 1979* and the Victorian *Surveillance Devices Act 1999* have been enacted to protect the individual's right to private communications by regulating the monitoring or recording of communications.

5.13 Under section 51(v) of the *Constitution*, the Commonwealth has power to legislate in relation to 'postal, telegraphic, telephonic and other like services'. This includes the power to legislate in relation to communications over a network. As a result, the *Telecommunications (Interception) Act 1979* (Cth) applies when a communication is in passage over a telecommunications system. Section 7 of the Act, subject to specific exceptions, prohibits a person from interception (by listening to or recording, by any means) a 'communication passing over a telecommunications system' without the knowledge of the person making the communication. In order to conduct surveillance, law enforcement and national securities agencies must obtain a warrant from a member of the Administrative Appeals Tribunal under Parts III, V or VI of the Act.

5.14 The Victorian *Surveillance Devices Act 1999* restricts the use of surveillance devices including optical devices, listening devices, tracking devices and data surveillance devices. It applies to interception of communications in circumstances not covered by the Commonwealth legislation, such as when a communication has ceased passage over a telecommunications system. Like the Commonwealth Act, it establishes a system of obtaining warrants in order to conduct surveillance which would otherwise be unauthorised. Victorian police are also authorised to obtain interception warrants in accordance with the Commonwealth legislation.[151] The *Surveillance Devices Act* is discussed in more detail in Chapter 6.

---

147 See Chapter 3.

148 See Chapter 3.

149 *Copyright Act 1968* (Cth).

150 The *Australian Postal Corporation Act 1989* (Cth) s 90 addresses issues such as employees opening, tampering with or stealing mail. See also *Crimes Act 1914* (Cth) Part VIIA.

151 *Telecommunications (Interception) (State Provisions) Act 1988* (Vic).

IS COMMUNICATIONS PRIVACY ADEQUATELY PROTECTED?

5.15 As communications technologies have become more sophisticated, so have technologies of surveillance. For example, radio frequency scanners can now be used to pick up and record some communications on cordless and mobile phones. Software programs can analyse a person's email and Internet usage, search for specific words, or even monitor communications using voice recognition systems to identify a particular individual across a network. Digital video surveillance cameras can constantly stream images over a telecommunications network. Information can be transmitted and stored on voice mail systems, ISP servers, computer hard drives, personal digital assistants, hidden cameras, concealed listening devices and pagers. As many of our new forms of communication – for example email, mailing lists and chat rooms - involve both a process of communication and a record of communications, the information communicated can be scanned, filtered, sniffed and stored before even being read by a recipient.[152]

CONCLUSION

5.16 The rise in the use of these technologies poses the biggest threat to communications privacy. As noted above, however, surveillance is an issue which extends beyond the scope of communications privacy. It is for this reason that, rather than discussing the specific adequacies of communications privacy protections in this Chapter, we examine the adequacy of our protection from surveillance as a whole in the next Chapter, focusing in particular on the *Surveillance Devices Act 1999* (Vic).

[152] See European Commission, Data Protection Working Party, *Privacy on the Internet: An Integrated EU Approach to On-line Data Protection*, 5063/00/EN/FINAL WP37, adopted on 21 November 2000, available at <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp37en.pdf>; Privacy Rights Clearinghouse, *Privacy in Cyberspace: Rules of the Road for the Information Superhighway*, Fact sheet 18, revised Aug 2000, available at <http://www.privacyrights.org/fs/fs18-cyb.htm>.

Chapter 6
Freedom from Surveillance

We are moving toward a surveillance society. Soon, government and private industry, often working in concert, will have the capability to monitor our every movement…While the technology is growing at light speed, the law that governs how the data can be used is developing at the speed of tortoises.[153]

BACKGROUND

6.1 Surveillance is becoming an increasingly important feature of modern life. People are watched in many ways. There is growing use of closed circuit television (CCTV) in public places such as shops, banks, workplaces, parking lots and streets. The use of surveillance for investigative purposes is also increasing.[154] Facial recognition technology takes surveillance networks a step further, making it possible to match photographs or video footage of individuals in a crowd to digital photographs contained in databases. This technology has been used to identify people in crowds at sports grounds[155] and is now gaining wider use. People's physical location and movements can also be tracked by the use of intelligent transportation systems that identify vehicles (and by association the owners of the vehicle). The e-TAG system utilised by Melbourne's CityLink road network makes it the first thoroughfare in the world that denies people the ability to travel anonymously.[156]

6.2 Groups that may have an interest in surveillance of people's physical location, movements, conversations and activities include:

- media organisations which use recordings from surveillance for news gathering purposes or entertainment purposes;

- employers who use surveillance to safeguard the security of property and staff, or to monitor the performance of employees;

---

153 Barry Steinhardt, Associate Director of the American Civil Liberties Union, quoted in A Sipress, '"Big Brother" Could Soon Ride Along in Back Seat' Washington Post, Sunday, October 8, 2000; Page A1.

154 The annual report on the *Telecommunications (Interception) Act 1979* for the year ended June 1999 reported growth in the number of warrants issued under Part VI of Act the from 675 to 1284, while the number rejected fell from 9 to 2: <http://www.law.gov.au/publications/annreptelecom.pdf>.

155 Such technology was used earlier this year at the US Super Bowl: see Peter Slevin, 'Focus on fans has them for and agin', *The Age*, 11 February 2001, available at <http://www.theage.com.au/news/2001/02/11/FFXMHN760JC.html>.

156 Roger Clarke, 'While you were sleeping' 2001, <http://www.anu.edu.au/people/Roger.Clarke/DV/AQ2001.html>.

- insurance assessors, private investigators and government agencies, who use surveillance to help investigate allegations of fraud when people make insurance claims or seek benefits under schemes such as WorkCover or TAC;

- community organisations which use surveillance for safety and welfare purposes;

- organisations which use surveillance as a deterrent against potential criminal activity, for example by installing Closed Circuit Television (CCTV) at train stations and 'trouble spots' like King Street, Melbourne;

- individuals who may use surveillance technologies to protect their own home and family against perceived threats to property and personal safety.

6.3 In this Chapter we focus largely on surveillance which monitors people's physical location, movements and activities, as this is the main area that has been the subject of legislative protection to date. However, it is important to recognise that the convergence of communications and information technologies, discussed in Chapters 4 and 5, has created the possibility for the increasing use of new forms of surveillance, including the tracking of people's transactions through their use of mobile phones and credit and debit cards. As noted in Chapter 5, electronic forms of communication create even more possibilities for surveillance. From employers monitoring their employees' emails to companies using cookies to track a person's movements around the Internet, almost every aspect of our electronic existence can be monitored. Electronic surveillance is often pervasive and indiscriminate. It is continuous, able to capture a substantial amount of personal information of innocent individuals, and it often occurs without any notice to the target, meaning that there is little accountability for the conduct of surveillance.[157] We will also briefly discuss these forms of surveillance in this Chapter.

HOW DOES THE LAW PROTECT US FROM SURVEILLANCE?

6.4 As discussed in Chapter 3, there are few common law remedies against surveillance. In general, the common law does not prevent activities which restrict the freedom of the individual to act anonymously and to move about unobserved. Because trespass and nuisance are primarily concerned with the protection of interests in land, they do not protect people from having their behaviour or movements scrutinised in public places.

6.5 In Chapter 5 we discussed legislation which provides some limited protection against surveillance of communications. In this Chapter we discuss the Victorian *Surveillance Devices Act 1999* which imposes criminal penalties on the unauthorised use, installation and maintenance of surveillance devices. These include optical surveillance devices (including cameras), listening

---

[157] Center for Democracy and Technology, Electronic Surveillance Task Force of the Digital Privacy and Security Working Group (Jun 1997) *Communications Privacy in the Digital Age: Interim Report*, available at <http://www.cdt.org/digi_tele/9706rpt.html>.

devices, tracking devices (which determine a person's location) and data surveillance devices used to record or monitor input of information into, or output of information from, a computer (such as devices which count key strokes).[158]

Restrictions on use, installation and maintenance of surveillance devices

6.6 Under the *Surveillance Devices Act*, unless authorised, the use, installation or maintenance of listening or optical surveillance devices to overhear private conversations or to observe private activities is usually prohibited.[159] For example, a private investigator who installed a device to record telephone calls or to film what occurred inside a house would be guilty of an offence under the Act. The Act also prohibits the installation or use of tracking devices to determine a person's location.[160] The people involved in the conversation or activity may, of course, consent to the use or installation of such devices. In addition, the Act allows a person to record a conversation to which they are a party regardless of the other party's knowledge or consent.[161] It would therefore be allowable, for example, to record a sexual encounter in which a person was involved without informing the other person.

6.7 There are various law enforcement exceptions to this general principle. Use, installation or maintenance of listening, optical surveillance, data surveillance or tracking devices without consent is permitted if it is authorised by a warrant or emergency authorisation under the Act[162] or under Commonwealth law.[163] In addition, a law enforcement officer can install an optical surveillance device on premises if this is authorised by the occupier of premises to protect their lawful interests.[164] This permits, for example, the installation of video surveillance in a workplace in order to prevent pilfering, without the consent or knowledge of employees.

Restrictions on use and publication

6.8 In Chapter 3, we saw that common law remedies for unauthorised intrusions onto private property do not always prevent publication of information obtained as a result of the intrusion. However, if the information has been obtained by using a surveillance device, the *Surveillance Devices Act* will prohibit the communication or publication of recordings or other records of private conversations or activities obtained, other than in specified circumstances.[165] A recording may only be published when:

- each party to the conversation consents; or

---

158 *Surveillance Devices Act 1999* (Vic) s 9.

159 *Surveillance Devices Act 1999* (Vic) ss 6, 7. Interestingly, while there are restrictions placed on law enforcement officers installing data surveillance devices (s 9), no similar restriction is placed on other people. It therefore seems acceptable, for example, for an employer to install a data surveillance device into an employee's computer.

160 *Surveillance Devices Act 1999* (Vic) s 8.

161 *Surveillance Devices Act 1999* (Vic) s 6(1).

162 *Surveillance Devices Act 1999* (Vic) Part 4.

163 *Surveillance Devices Act 1999* (Vic) ss 6-8.

164 *Surveillance Devices Act 1999* (Vic) s 7(2).

165 *Surveillance Devices Act 1999* (Vic) s 11.

- publication is in the public interest (covering some news gathering activities); or
- publication is for the protection of the lawful interests of the person who made the recording; or
- publication occurs in the course of legal or disciplinary proceedings; or
- publication occurs in certain law enforcement or national security situations.

6.9 This prohibition applies to all recordings of private conversations or activities including those lawfully obtained by a party to the conversation or activity. While it is therefore possible for a person to secretly film a sexual encounter in which they are involved, they cannot publicly screen that film without the consent of the other person. This provides some protection to private communications. However, it does not protect people from the publication of information obtained without the use of surveillance devices.

IS THE PROTECTION AGAINST SURVEILLANCE ADEQUATE?

6.10 The *Surveillance Devices Act 1999* (Vic) provides only piecemeal privacy protection for individuals. The Act does not provide adequate protection from surveillance for the reasons discussed below.

Restricted definitions of 'private conversation' and 'private activity'

6.11 While the *Surveillance Devices Act* recognises that private conversations ought to be protected from eavesdropping, 'private conversation' is defined in the Act to exclude conversations that might be overheard by someone else.[166] This means that many activities that participants might reasonably expect to be private are not protected. For example, an acrimonious conversation in a backyard which could be overheard by neighbours, or an intimate conversation in a restaurant overheard by a waiter, are likely to be excluded because in both cases the conversation may be overheard by someone else. The Act will not prevent these conversations from being surreptitiously recorded and then publicised.

6.12 Similarly, individuals are protected from the surveillance of private activities but 'private activity' has a restrictive definition. The protection against video surveillance does not extend to an activity that takes place outside a building or an activity where the parties ought reasonably expect that it may be observed by someone else.[167] Again, many activities that people might reasonably expect to be private (and therefore not subject to covert recording and publicity) are in fact not protected by the Act. For instance, sunbathing in your backyard is not covered as the activity takes place outside a building. Similarly, activities taking place in your home that are visible from the street or a neighbouring apartment (through a window) are not protected from surveillance (and publication).

---

[166] *Surveillance Devices Act 1999* (Vic) s 3.

[167] See definition of 'private activity': *Surveillance Devices Act 1999* (Vic) s 3.

6.13 Interestingly, the Explanatory Memorandum to the Act identifies as private those activities which take place in toilet cubicles and changing rooms on the basis that it is reasonable to believe that they would take place unobserved by another person. It is questionable, however, whether the Act extends privacy protection to activities that take place under more 'public' or 'exposed' circumstances. For example, a video recording of men in front of a urinal rather than in a cubicle, or of children in a school gym or in the toilet of a day care centre, may not be covered by the Act.

Use of biometric technologies may not be covered

6.14 While the Act regulates the use of tracking devices to determine the *geographical location* of people, it does not restrict the use of technologies which can be used to identify people in public or private places. Biometric technologies such as retina scans, voice recognition software, face recognition software, thumb scans and fingerprints may be required as a condition of access to certain places or services or within workplaces. One function of these technologies is to determine people's identities. While use of such technologies may be justified in certain situations, the accumulation of information as a result of their pervasive use increases social control and significantly restricts people's ability to participate in everyday activities anonymously.

Use of different forms of surveillance may not be covered

6.15 In recent years increased concern has been raised about the interception of communications by intelligence services and national security agencies. Revelations of a global satellite system for the interception of private and commercial communications, known as the Echelon interception system, have recently sparked vigorous debate in Europe[168] along with the Council of Europe's Draft Convention on Cyber-Crime.[169] Revelations of the Federal Bureau of Investigation's Carnivore e-mail surveillance network have similarly sparked controversy in the United States.[170] These issues raise concerns about the technical and legal capability of law enforcement and national security agencies to conduct surveillance of communications and the degree to which these agencies are accountable in how they exercise their functions.

6.16 Critics have argued that systems such as Echelon, in which Australia is an acknowledged participant, breach the ICCPR provision against unlawful and arbitrary interference with privacy given that they involve indiscriminate surveillance of personal communications without any prior grounds for suspicion. Despite this, it is unlikely that the *Surveillance Devices Act* can provide any remedies against such surveillance. This will partly be because of the nature of the surveillance which uses satellite and other advanced forms of technology which may not fall within the scope

---

168 See, eg, *Draft Report of the European Parliament's Temporary Committee on the Echelon Interception System* available at <http://www.europarl.eu.int/tempcom/echelon/pdf/prechelon_en.pdf>.

169 Information on the Cyber-Crime Convention is available at <http://www.privacyinternational.org/issues/cybercrime/index.html#coe>.

170 The United States Justice Department responded to these criticisms by appointing an independent inquiry, the final report of which is available at <www.usdoj.gov/jmd/publications/carniv_final.pdf>. An overview of similar government surveillance systems in other countries can be found at 'Echelon Watch', a web site administered by the American Civil Liberties Union in conjunction with the Free Congress Foundation, the Electronic Privacy Information Center, Cyber-Rights and Cyber-Liberties (UK) and the Omega Foundation, available at <http://www.aclu.org/echelonwatch/networks.html>.

of optical or listening devices. In addition, the nature of the agencies themselves is likely to preclude remedies – either because, as intelligence agencies, they are excluded from the scope of the laws, or due to jurisdictional problems.

6.17 Similarly, the *Surveillance Devices Act* seems ill-equipped to deal with many electronic forms of surveillance. As noted in Chapter 5, it is now possible to monitor people's communications by the use of cookies, web-bugs and filtering or sniffing programs. None of these methods of surveillance involve the physical installation of the 'devices' prohibited by the Act and so fall outside its scope.

6.18 Unfortunately, in each of these cases, given the nature of the surveillance, effective regulation would require federal, if not international, measures. As a result, the Commission does not intend to focus on these types of surveillance.

Lack of real consent

6.19 Several provisions within the *Surveillance Devices Act* permit surveillance with the 'express or implied' consent of the individual subjected to it. There are practical problems with provisions which state that surveillance is permitted with the consent of individuals, when individuals often have no real capacity to refuse. For example, a person seeking entry to a shopping mall or a sporting ground, purchasing food or petrol, taking public transport, or participating in the workplace as an employee, has no real choice as to whether or not they are placed under surveillance. This suggests that the normal model of relying on informed choice to protect an individual's privacy cannot address the privacy issues arising from widespread public surveillance.

Lack of control of surveillance in public places

6.20 The *Surveillance Devices Act* conceives privacy as something that is sacrificed as soon as you leave your home or interact in a place frequented by other people. For instance, there are no restrictions in the Act on video surveillance in public places or quasi-public places outside buildings. Nor does the Act prevent a private investigator from installing a video camera in a street to monitor people entering or leaving a building.

Problems with workplace surveillance

6.21 The limited protection provided by the *Surveillance Devices Act* is of particular concern when considering privacy invasions in workplaces. While employers have legitimate interests in using surveillance to protect their property rights, such as by detecting dishonest workers and ensuring worker safety, intrusive surveillance is becoming increasingly frequent in workplaces for other purposes, such as monitoring employee performance.[171] The *Surveillance Devices Act* does not specifically regulate workplace surveillance or give employees more protection than that available to people in public places. Employers can install and monitor various surveillance technologies

---

[171] See, eg, J Sempill, 'Under the Lens: Electronic Workplace Surveillance' forthcoming Australian Journal of Labour Law. In 1995, the New South Wales Privacy Committee released a report, *Invisible Eyes: Report on Video Surveillance in the Workplace*, which discussed these issues and later led to the passage of the *Workplace Video Surveillance Act 1998* (NSW).

without breaching the Act, either because a worker's conversations and activities do not fit the definitions of 'private conversation' or 'private activity',[172] or because employers require employees to consent to surveillance as a condition of their employment. In addition, it seems that employers can use data surveillance devices such as devices to count key strokes into a computer without restriction.[173]

6.22 In contrast, the New South Wales *Workplace Video Surveillance Act 1998* requires employers to obtain court approval to install covert video surveillance and permits such surveillance only for the purposes of detecting unlawful activity.[174] Covert surveillance is not permitted at all in some private areas, for example toilets, showers and change rooms.[175] Covert surveillance must also be overseen by a licensed security officer who can only supply the employer with parts of the tape which are relevant to establish the existence of unlawful activity.[176] Parts of a record of surveillance not required for evidentiary purposes must be erased or destroyed within three months.[177] While the New South Wales Act is not perfect[178] it at least attempts to deal with workplace specific issues that are not addressed in the Victorian Act.

Problems arising from mass surveillance

6.23 A major weakness in the legislation is that it does not take into account the realities of contemporary surveillance technologies and does little to prevent mass surveillance. The legislation regulates *how* surveillance is conducted but does not limit the purposes for which it can be used. While the *Surveillance Devices Act* regulates surveillance on a small scale and by law enforcement officers, it does not limit its use on a large scale in public and semi-private places, either by the state or by ordinary citizens and organisations. Some privacy experts argue that such forms of regulation in fact serve to *legitimise* the conduct of surveillance[179] rather than protect privacy by preventing the establishment of surveillance networks in the first place. In other words, privacy laws may 'correct the mistakes and misuses but [they do] not attack the way in which technology is used'.[180]

---

172 See above.

173 Limitations are only placed on the use of such devices by law enforcement officers: *Video Surveillance Act 1999* (Vic) s 9.

174 *Workplace Video Surveillance Act 1998* (NSW) ss 7 and 10. Note that 'covert surveillance' is defined in s 4 of the Act.

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

176 *Workplace Video Surveillance Act 1998* (NSW) ss 17(1)(a)-(b) and 18.

177 *Workplace Video Surveillance Act 1998* (NSW) s 17 (1)(C).

178 Of particular concern is the distinction drawn in the Act between 'overt' and 'covert' surveillance. While covert surveillance is closely regulated, overt surveillance does not come under the same scrutiny. The traditional argument in favour of maintaining such a distinction is that if a person knows they are being surveilled, and accepts such surveillance, they have impliedly consented to it. As noted above, however, such consent is often not genuine – people may feel they have no choice but to comply. This will particularly be the case in the context of the workplace, where people may not wish to jeopardise their job security.

179 One of the strongest criticisms of privacy laws is that privacy agencies 'simply become agents for legitimating information-collection activities': D Flaherty, *Protecting Privacy in Surveillance Societies*, University of North Carolina Press, 1989, p 384.

180 J Holvast, 'Vulnerability of information society' in R Clarke and J Cameron, *Managing Information Technology's Organisation Impact*, North Holland, Amsterdam, 1991.

CONCLUSION

6.24 This Chapter has outlined the limited protection available against surveillance. This lack of protection is of particular concern given the ready availability of surveillance technologies at a much lower cost than in the past. This has extended the availability of surveillance technologies from law enforcement and national security agencies to private organisations and ordinary citizens, increasing the use of such technologies in all aspects of society from the streets to the workplace.

6.25 The regulation of mass surveillance in public places is a substantial gap in the privacy protection offered in Victoria, as is the use of surveillance by employers. Extensive surveillance without limitations has the potential to significantly effect the nature of a free society. Abuse of these technologies may severely damage the lives of individuals as well as making us all feel less free. At the same time, used responsibly, surveillance may offer greater protection for individuals' personal safety and property. Finding a balance between these interests is an important challenge. The Commission believes that the regulation of mass surveillance and of surveillance in the workplace are priority areas for reform within Victoria.

Chapter 7
Workplace Privacy

> *Defining an appropriate zone of privacy in the workplace is being undertaken through legal developments in all the countries examined in this [report]. The development of workers' privacy rights is tempered by employer prerogative to control what goes on in the workplace and the performance of employees and to protect and control the employer's property.*[181]

BACKGROUND

7.1 In earlier Chapters in this Paper we have identified gaps in existing protection for bodily, territorial, information and communications privacy, as well as on the lack of protection against surveillance. These gaps may have a particularly serious effect on employees. This may be because a privacy–invasive technology is used in the workplace before it is used elsewhere; it may be because of the extensive nature of the surveillance from which the employee cannot escape; or it may be because employees are under greater pressure to agree to privacy invasions than people outside the employment context. As people increasingly work from home these technologies can reach beyond the work environment into people's personal lives creating an even greater impact on employee privacy.

7.2 Current workplace practices which may effect employee privacy include the use of:

- drug and alcohol testing;
- psychological testing;
- biometric devices to monitor the movement of employees in their workplaces or elsewhere;
- technology which monitors employee communications such as the use of emails, the internet, or mobile phones;
- devices to monitor the keystroke speed of computer operators; and
- overt or covert video and audio surveillance.

7.3 There are a number of reasons why employers may implement such privacy-invasive practices. For example, video surveillance may be used to detect theft, vandalism or misconduct,

---

[181] International Labour Organisation, Conditions of Work Digest: Workers' Privacy Part II – *Monitoring and Surveillance in the Workplace*, p 9.

or to reduce security and liability risks. Employers may also find it desirable to use privacy-invasive technologies to monitor the performance of employees, to increase productivity and to prevent employees wasting work time. However, from an employee's perspective, strategies which deny them a reasonable level of privacy in the workplace and de-humanise their working environment may be used to harass them and may produce intolerable levels of stress. Workplace privacy raises difficult questions about the appropriate balance to be struck between employers' claims to exercise management and control over workers, and the rights of employees to have their autonomy and privacy respected and to be treated with dignity.

HOW IS PRIVACY IN THE WORKPLACE PROTECTED?

7.4 There are no Victorian or Commonwealth laws which deal generally with the issue of workplace privacy, although anti-discrimination legislation may prevent the discriminatory use of information relating to issues such as race, disability, sexuality and past convictions for the purposes of employment-related decisions.[182] Each of the areas outlined in Chapters 2-6 may, however, offer incidental protection for workplace privacy. In certain circumstances, for example, actions for assault and battery or trespass may provide some relief to employees – although, as outlined below, there are substantial gaps in the protections offered.

7.5 When the federal *Privacy Act* was amended in 2000 the Government announced that the Attorney-General's Department and the Department of Employment, Workplace Relations and Small Business would conduct a review of the extent of privacy protection for employee records in existing Commonwealth, State and Territory laws to see whether there was a need for further regulation. At the same time it also announced that it would leave the handling of workplace privacy issues to industrial relations laws.

7.6 However, industrial relations laws do not at present deal with privacy issues in any substantial way. For example, although under section 353A of the *Workplace Relations Act 1996* (Cth) the government may make regulations relating to employee records, the current regulations under this provision mainly require employers to maintain records about the conditions under which an employee is hired and to maintain information concerning their working hours.[183] There is no specific reference to maintaining the privacy of those records.

7.7 The current industrial relations framework has limited capacity to deal specifically with privacy issues without legislative change. The Australian Industrial Relations Commission does not have the power to establish provisions for workplace privacy through the award system.[184] While it would be possible to deal with privacy issues in enterprise bargaining agreements,

---

182 See, eg, *Equal Opportunity Act 1995* (Vic); *Disability Discrimination Act 1992* (Cth); *Racial Discrimination Act 1975* (Cth); *Sex Discrimination Act 1984* (Cth); *Crimes Act 1914* (Cth) Pt VIIC.

183 Regulation 131L(1) does require employers to make a copy of a record available on request by an employee or former employee to whom the record relates. Regulation 131M provides that an employer must inform an employee of the location of the record which they are requesting, and make the record available within a maximum of 14 days after the request.

184 The Australian Industrial Relations Commission's jurisdiction relating to awards is limited to 20 allowable matters, which do not include privacy issues.

Australian Workplace Agreements or individual employment contracts, in practice the use of monitoring technologies in the workplace is usually the result of unilateral decisions by employers rather than an outcome of employer-employee consultation. In addition, given the inequality of bargaining power between employers and employees it is unlikely that there would be a genuine capacity to negotiate over such issues.

7.8 In response to concerns about the erosion of privacy in the workplace, some countries have addressed workplace privacy issues through a general law or code of practice. The United Kingdom's Information Commissioner released a draft Employment Code of Practice in October 2000 which attempts to deal comprehensively with the issues relating to surveillance of employees.[185] The Hong Kong Privacy Commissioner for Personal Data has also been developing a code on workplace surveillance.[186] The only significant response in Australia has been the New South Wales *Workplace Video Surveillance Act 1998* which addresses specific employee privacy issues through legislation.[187] The New South Wales Law Reform Commission has also recently reported on workplace surveillance but this Report has not yet been made public.[188]

IS THERE ADEQUATE PROTECTION OF WORKPLACE PRIVACY?

7.9 As noted above there are no specific laws to protect workplace privacy. While the laws protecting privacy of the body, physical space, information, communication and freedom from surveillance may offer some protection for employees, previous chapters have identified a number of workplace-specific gaps:

- Remedies for assault and battery do not apply if an employee *consents* to a blood or urine test. In the workplace context, it is unlikely that employees will feel free to refuse such consent.

- Assault and battery do not provide a remedy for indirect invasions of bodily privacy, for example by the use of biometric or psychometric techniques.

- Laws protecting people's privacy in physical space do not protect employees against invasions of privacy by their employer while on the employer's premises. Employees may also have little choice about consenting to activities such as searches of their possessions.

- Personal information provided in the employment context is not adequately protected. Although the *Privacy Act 1988* (Cth) has been extended to cover the private sector, employee records are exempt from privacy protection.[189]

---

185 See <http://www.dataprotection.gov.uk>.

186 See <http://www.pco.org.hk>. An overview of workplace privacy laws is to be provided in a forthcoming report on workplace surveillance to be issued by the Hong Kong Privacy Commissioner for Personal Data.

187 See Chapter 6.

188 For further information see the speech notes of Attorney-General Bob Debus available at <http://www.oznetlaw.net.>.

189 *Privacy Act 1988* (Cth) s 7B(C). Particular types of information about employees, such as health record information, may be protected by specific State laws such as the Victorian *Health Records Act 2001*.

- There are no clear limits on the power of employers to monitor employee communications such as email.
- There appear to be no restrictions on the use of data surveillance devices, such as key-stroke monitors, by employers in Victoria.
- Due to the narrow definition of 'private activities' and 'private conversations' in the *Surveillance Devices Act 1999* (Vic), employers can use covert or overt surveillance devices to monitor performance in most areas of a workplace. With an employee's consent, this could include surveillance in the employee's home.

CONCLUSION

7.10 Existing Australian law gives employees very limited privacy protection. Given the number of people potentially affected by workplace privacy invasions and the serious impact such invasions can have, the Commission believes this is a priority area for law reform. The reference could relate to workplace privacy in general or could examine particular aspects of the problem, such as workplace video surveillance. The disadvantage of focusing on specific areas is that this would result in a piecemeal approach to the problem of workplace privacy. However, this may be inevitable to some extent as there will be certain issues which it may not be possible to deal with at a State level due to potential conflict with Commonwealth laws.[190] Any reference on workplace privacy would need to carefully consider the inter-relationship between State and Commonwealth laws.

[190] One example may relate to aspects of communications privacy, over which the Commonwealth has power under the *Constitution* s 51(v). Other conflicts may arise in relation to the Commonwealth's power to make laws in relation to 'conciliation and arbitration for the prevention and settlement of industrial disputes extending beyond the limits of any one State': *Constitution* s 51(xxxv). In addition, most aspects of Victorian industrial law have been referred to the Commonwealth, although this reference of powers is revocable: *Commonwealth Powers (Industrial Relations) Act 1996*.

Chapter 8
Conclusion

8.1 Throughout this Paper we have examined the ways in which the law protects the privacy of the body, physical space, information and communications, as well as rights to freedom from surveillance. In each of these areas we have identified some important gaps in the extent to which the present law protects the privacy of individuals. We have highlighted the following areas as lacking sufficient protection:

- the privacy of the body, in light of the expanding and wide-ranging powers of the police and other investigatory authorities;
- the privacy of the body from biometric and psychometric technologies;
- genetic privacy;
- privacy in public places;
- the privacy of employees' physical space and personal belongings;
- the privacy of information obtained as a result of invasions of physical space;
- the privacy of private sector employee records;
- the privacy of information held on public registers; and
- freedom from surveillance in a variety of situations, including public places and the workplace.

8.2 In Chapter 1 we identified some principles which could be used to prioritise the areas for the Commission's work on privacy law reform. These were:

- whether investigation of the issue would involve duplicating work already being undertaken by other law reform bodies;
- whether the issue would be more appropriately dealt with at a Commonwealth level;
- whether existing privacy legislation has been in operation for a sufficient time for us to assess its impact; and
- the seriousness of the privacy problem which is being considered.

8.3 In light of these principles, the Commission has tentatively concluded that the following areas would not be appropriate avenues for our focus at this time:

- **Police powers:** this raises civil liberty issues which extend beyond the scope of concerns about privacy.

- **Other investigatory authorities:** the Victorian Parliamentary Law Reform Committee is currently examining the limits on the powers of investigatory bodies other than the police.

- **Genetic privacy:** the Australian Law Reform Commission and the Australian Health Ethics Committee are currently examining this issue.

8.4 Except in the case of public registers, which is discussed below, we have also argued that it would be inappropriate for the Commission to focus on the coverage of the Victorian *Information Privacy Act*, as the Privacy Commissioner has only just been appointed and the Act is not yet in force. Some time will be necessary to assess the effectiveness of the legislation and ascertain the problem areas.

8.5 We have suggested that areas which could be given priority include:

- the gaps in privacy protection for publicly available information such as information held in public registers;

- the problems arising from the pervasive use of surveillance technology, especially in public places and in workplaces;

- the lack of adequate privacy protection for employees. This could include issues ranging from surveillance of employees and their communications to the use of biometric and psychometric technologies. Other potential avenues for investigation include the protection of employee records and the privacy of employee's physical space and personal belongings.

8.6 In considering priorities for the Commission's work, it is important to identify the roles that the Commonwealth and State governments may play in the future reform of privacy law. The Commonwealth power to legislate to implement Australia's treaty obligations gives it relatively broad powers to protect privacy.[191] The Commonwealth could also make privacy-related laws under its trade and commerce, posts and telegraphs, conciliation and arbitration, banking, corporations and insurance powers.[192] The current referral of many of Victoria's industrial relations powers to the Commonwealth[193] would also enable it to make workplace-related privacy laws.

8.7 To date, the Commonwealth has focused on protecting information privacy and some aspects of communications privacy. As we have seen, the *Workplace Relations Act 1996* (Cth) does not deal in detail with employee privacy. Issues relating to public registers held by State agencies

---

191 *Constitution* s 51(xxix).

192 *Constitution* ss 51(i), (v), (xxxv), (xiii), (xx), (xiv).

193 *Commonwealth Powers (Industrial Relations) Act 1996* (Vic).

and surveillance fall within areas of legislative power traditionally exercised by the States. General issues of workplace privacy could be dealt with by either State or Commonwealth legislation, though a joint Commonwealth/State approach would probably be the most effective.

This paper seeks views as to the areas which should be included in a reference to the Victorian Law Reform Commission.

Appendix A
Glossary

BIOMETRICS

Techniques of personal identification that are based on physical characteristics. Biometric techniques include fingerprinting, ***retinal scanning*** and ***voice recognition.***

BREACH OF CONFIDENCE

A legal action based on the failure to preserve the confidential character of information communicated in confidential circumstances.

CHAT ROOM

A site on a computer network where a number of users can meet and interact in real time.

CIVIL LAW

Non-criminal law. Civil law generally involves legal proceedings brought by one person against another. Examples include negligence, battery or breach of copyright.

CLOSED-CIRCUIT TELEVISION (CCTV)

A television system that feeds camera transmissions directly to monitors in nearby locations – typically used for visual surveillance of places and activities.

COMMON LAW

A body of law which comes from cases decided by judges rather than from laws made by Parliament.

COOKIES

A small file placed on a user's computer hard drive used to store information about a user when visiting a website. This file can then be accessed and read by the website at each return visit.

Cookies are used for purposes such as allowing users to re-visit a site without having to re-enter login names and passwords, storing lists of items the user selected on an earlier visit to a virtual store (such as the online bookstore, Amazon.com) or tailoring products or advertisements to the user's interests.

CYBERSPACE The electronic 'space' or 'place' created by computer networks where online activities take place; often contrasted with the physical world where 'offline' or 'real life' activities occur.

DATA SURVEILLANCE DEVICE Defined in section 3 of the *Surveillance Devices Act 1999* (Vic) as 'any device capable of being used to record or monitor the input of information into or the output of information from a computer, but does not include an optical surveillance device'. A device that enables the number of keystrokes typed would be a data surveillance device.

EMPLOYEE RECORDS Defined in section 6(1) of the *Privacy Act 1988* (Cth) to include employees' health information; personal and emergency contact details; terms and conditions of employment; salary; trade union membership; taxation, banking or superannuation details.

FACE RECOGNITION SOFTWARE A computer program that matches images of people captured by photograph or video recording (such as from surveillance cameras) with facial images stored in computer databases.

FILTERING The use of computer hardware and/or software to sort or block websites or email. For example, a filtering program may prohibit access to any website containing the word 'sex'.

HACKING To gain access to a computer file or network illegally or without permission.

HAND GEOMETRY A ***biometric*** technique that uses the geometric shape of the hand to authenticate a person's identity.

INJUNCTION A court order requiring a party to do, or refrain from doing, a specified act.

INTERNET SERVICE PROVIDER (ISP) A company that provides people with access to the Internet.

LISTENING DEVICE

Defined in section 3 of the *Surveillance Devices Act 1999* (Vic) to mean any device that can monitor or record a private conversation, but not including a hearing aid.

MAILING LIST

An email discussion forum where participants subscribe to a particular group (a 'list'), receive copies of messages sent by other members of that group, and can email their own message for forwarding to the group. Some mailing lists are moderated by a person who will receive all emails, screen them and decide which ones to publish. Unmoderated lists simply forward all emails received to the group of subscribers.

NEWSGROUP

A subject-based discussion forum on the Internet which takes place by people posting messages for everyone to read. Like ***mailing lists***, newsgroups can be moderated or unmoderated.

OPTICAL SURVEILLANCE DEVICE

Defined in section 3 of the *Surveillance Devices Act 1999* (Vic) to mean any device that can be used to visually monitor or record a private activity, but not including glasses or contact lenses.

PARTICIPANT MONITORING

The monitoring (by recording or transmitting) of a conversation or activity in which one participates personally. Participant monitoring can be overt or covert.

PROFILING

The compilation of information, usually from a variety of sources (such as Internet sites visited, items purchased, public records), to create a profile of a particular individual. This profile is often used to market products to that individual.

PSYCHOMETRICS

Techniques to measure and analyse psychological functions. Psychometric techniques include psychological testing, personality testing and intelligence testing.

PUBLIC RECORDS The records of organisations that are accessible by the general public. Examples include court records and planning applications held by local councils.

PUBLIC REGISTERS Public registers are lists that are required to be made available to the public by legislation or regulation. Examples include the Motor Vehicle Register, the Land Titles Register, and the Births, Deaths and Marriages Register.

PUBLICLY AVAILABLE INFORMATION Information that the general public can access. Examples include information contained in newspapers, professional directories and genealogical databases.

QUASI-JUDICIAL The actions of non-judicial bodies exercising their powers and functions in a judicial manner. Examples of non-judicial bodies include tribunals and administrative agencies.

RETINAL SCAN A ***biometric*** technique that uses light to measure patterns in the retina (at the back of the eyeball) to authenticate a person's identity.

SEARCH ENGINE A remotely accessible computer program that enables keyword searches for information on the Internet to be performed.

SNIFFING The use of computer hardware and/or software to search for designated keywords. For example, a sniffing program could be used to search a person's email for any mention of the word 'drugs'.

TRACKING DEVICE Defined in section 3 of the *Surveillance Devices Act 1999* (Vic) to mean 'an electronic device the primary purpose of which is to determine the geographical location of a person or an object'.

TRANSBORDER DATA FLOW The movement of information or computer data across national or state boundaries.

UNIQUE IDENTIFIER

Defined in Schedule 1 of the *Information Privacy Act 2000* (Vic) to mean 'an identifier (usually a number) assigned by an organisation to an individual uniquely to identify that individual for the purposes of the operations of the organisation but does not include an identifier that consists only of the individual's name'.

VOICE RECOGNITION SOFTWARE

A computer program that recognises speech. Uses of voice recognition software include identifying the speaker and searching conversations for specified words or phrases.