NSW PARLIAMENTARY LIBRARY RESEARCH SERVICE

Privacy: The Current Situation

by

Jason Arditi

Briefing Paper No 7/08

RELATED PUBLICATIONS

- *Workplace Surveillance* by Lenny Roth, NSW Parliamentary Library Briefing Paper No 13/2004
- *Information Privacy and Health Records* by Gareth Griffith, NSW Parliamentary Library Briefing Paper No 6/2002
- *Privacy Law Reform: Issues and Recent Developments* by Gareth Griffith, NSW Parliamentary Library Briefing Paper No 20/1998
- *Privacy an Data Protection Law Reform: Some Relevant Issues* by Gareth Griffith, NSW Parliamentary Library Briefing Paper No 15/1996
- *The Individual's Right to Privacy: Protection of Personal Information in New South Wales* by Vicki Mullen, NSW Parliamentary Library Briefing Paper No 14/1995

ISSN 1325-5142
ISBN 978 0 7313 1838 4

July 2008

Privacy:
The Current Situation

by

Jason Arditi

NSW PARLIAMENTARY LIBRARY RESEARCH SERVICE

David Clune (MA, PhD, Dip Lib), Manager……..……(02) 9230 2484

Gareth Griffith (BSc (Econ) (Hons), LLB (Hons), PhD),
Senior Research Officer, Politics and Government / Law…….(02) 9230 2356

Jason Arditi (BA, LLB) Research Officer, Law……..…(02) 9230 2768

Tom Edwards (BSc (Hons)), Research Officer, Environment……...(02) 9230 3085

Kathryn Simon (BA, LLB (Hons), LLM) Research Officer, Law……..…..(02) 9230 2003

Stewart Smith (BSc (Hons), MELGL), Research Officer, Environment.…….(02) 9230 2798

John Wilkinson (MA, PhD), Research Officer, Economics……..(02) 9230 2006

Should Members or their staff require further information about this publication please contact the author.

Information about Research Publications can be found on the Internet at:

www.parliament.nsw.gov.au/WEB_FEED/PHWebContent.nsf/PHPages/LibraryPublications

CONTENTS

EXECUTIVE SUMMARY

This *Briefing Paper* looks at the development of personal information privacy law in New South Wales. It examines the historical context in which privacy emerged as a significant concern that warranted statutory protection and regulation. **[1] – [2]**

The paper commences by identifying the imprecise nature of concepts of privacy and difficulties in providing a comprehensive definition. Consideration is then given to the different categories of privacy that combine to give the overall theme of privacy character and content. **[3]**

Following on from this, the paper briefly touches on the obligations under international law relating to privacy and how that, together with domestic issues, had an influence on privacy legislation in Australia. **[4] – [6]**

The paper then provides a brief examination of the Privacy Act, including the Information Protection Principles, the code that forms the basis of privacy law in New South Wales. It then turns to the possible development of the tort of privacy at common law, with some reference to foreign jurisprudence and a possible statutory tort of privacy. **[7] – [9]**

Some of the issues regarding the patchy and fragmented nature of the privacy regime in Australia are discussed before a brief assessment of new and emerging technologies that are potentially privacy-intrusive. **[10 – 13]**

1 INTRODUCTION

This *Briefing Paper* looks closely at what privacy is and examines its legal development in New South Wales. The paper also touches on some of the concerns facing privacy, both from the regulatory standpoint and through changes brought about by technological progress.

Privacy is a largely elusive concept that has proven to be notoriously difficult to define.[1] As, such, it has been argued that privacy is a value better experienced than defined.[2]

The word 'privacy' is derived from the Latin root *'privare'* meaning, to deprive of access to the public sphere. That is, to be separate, secluded and free from the unwanted intrusion of others. [3] The genesis of the modern concept of privacy viewed through the legal prism can be found in the landmark article written by Louis Brandeis and Samuel Warren in 1890, 'The Right to Privacy'. In it, Brandeis and Warren argue that privacy is, fundamentally, 'the right to be let alone'. [4]

In its 1983 report on privacy, the Australian Law Reform Commission elaborated on Brandeis and Warren's initial definition to describe privacy as 'part of the claim that the autonomy of each individual should be protected and his integrity respected.'[5] The report found the privacy involves numerous aspects, including:

- that the person of the individual should be respected, that is, not interfered with, without consent;
- that the individual should be able to exercise a measure of control over relationships with others, including the ability to exercise an appropriate measure of control on the extent to which his / her correspondence, communications and activities are available to others in the community;
- that the individual should be able to control the extent to which information about him / her is available to others in the community.[6]

The nebulous nature of privacy is such that it means different things to different people with many factors influencing personal perceptions. For some, privacy is fundamentally about maximising his or her own anonymous space and limiting what other people can observe. To others, it is about control of their personal information, to whom it is disclosed and who has access to it. In some respects, privacy is culturally relative, with what may be considered

---

[1] See Raymond Wacks, *Personal Information,* Oxford University Press, 1989 at p 13 – 18.

[2] Brett Mason, *Privacy without principle: The use and abuse of privacy in Australian law and public policy,* Australian Scholarly Publishing, Melbourne 2006 at p 1.

[3] Moira Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State,* LexisNexis Butterworths 2005 at p 15.

[4] LD Brandeis and SD Warren, 'The right to privacy' (1890) *4 Harvard Law Review* 193 at p 195.

[5] Australian Law Reform Commission, *Privacy,* paras 1032 -1033.

[6] Ibid.

privacy-intrusive behaviour in some cultures accepted as appropriate in others.[7]

Similarly, the degree of importance ascribed to privacy varies according to individual values and circumstances. For some, openly disclosing intimate aspects of their personal lives and being recorded on camera may not be concerning. For others, however, even the mere disclosure of a phone number can be considered an egregious interference with their privacy. This might be especially so if that person is concerned about receiving unsolicited marketing calls or, more importantly, has concerns for their security as a result of their phone number being disclosed.

Privacy is therefore a highly personal quality and how we define it, together with the importance we place on it, is highly subjective.

Privacy is also time relative. A century ago, protecting oneself from interferences to privacy may have been as simple drawing a curtain or closing a door. Today, advances in technology and its increasing popularity have added stress to privacy and further complicated the ways in which we can protect privacy.[8]

2 PRIVACY AS A HUMAN RIGHT?

The Australian Privacy Charter states:

> People have a right to privacy of their own body, private space, privacy of communications, information privacy (rights concerning information about a person) and freedom of surveillance.[9]

Whether or not privacy itself is a 'right' as such, has also been the subject of considerable academic debate. Some have regarded privacy as one of many human *interests* that must compete in a marketplace against other equally valid but sometimes conflicting interests. In its 1983 report on privacy, the ALRC noted that privacy interests are not absolute, but must be weighed against other interests.[10] The Office of the Privacy Commissioner has also noted that a balance has to be achieved between the needs of the individual and the broader community.[11]

Alternatively, it has been argued that privacy is a human right, on par with the most fundamental of human rights and cannot be abrogated or varied merely for convenience's sake. This argument is backed up by the fact that privacy is proclaimed as a right under article 12 of the Universal Declaration of Human Rights.[12]

---

[7] Victorian Law Reform Commission, *Privacy Law: Options for Reform Information Paper,* July 2001 at p 3.

[8] Ibid.

[9] Preamble to the Australian Privacy Charter at http://www.privacy.org.au/About/PrivacyCharter.html, accessed 7 July 2008.

[10] Law Reform Commission, *Privacy*, ALRC Report No. 22, Volume 1, 1983 at p 20.

[11] *Committee Hansard,* 19 May 2005, p. 51 in Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988,* June 2005 at p 8.

[12] The Universal Declaration of Human Rights, http://www.un.org/Overview/rights.html, accessed 7 July 2008.

A compromise position between privacy as a 'right' and an 'interest' is that privacy is a right, but one that does not rank highly in the hierarchy of rights.[13]

3 CATEGORIES OF PRIVACY

A better understanding of privacy can be achieved by examining four separate, yet related, categories. Although different, each category touches on certain aspects of what is commonly understood to refer to privacy.

3.1 Surveillance

Surveillance is defined as 'the systematic observation or recording of one or more people's behaviour, communication, or personal information'.[14] In its most basic form, surveillance is about 'peeping toms' and eavesdroppers. However, technological progress has meant that surveillance today is more about the visual and audio recordings of an individual and his or her conversations or actions: CCTV, for example, streams footage of people in the public domain and tracking what Internet sites a person has visited from the comfort of their home computer. In the extreme, surveillance is epitomised by George Orwell's dystopian society in '1984' and the notion of the all-intrusive 'Big Brother', ubiquitously observing the movements of subjects under its control. Naturally, in a free society, people want to go about their daily lives free from the prying eyes and ears of others and a healthy society maximises the ability in which an individual can retain a fair degree of anonymous space.

Surveillance privacy is largely regulated separately from other forms of privacy (notably, information privacy) and in New South Wales has been covered by various Acts. Surveillance privacy law is designed to ensure that individuals are reasonably able to go about their lives without being tracked and, if they are tracked for legitimate reasons, then ensuring the collection of the information that has been intercepted is appropriately handled.

In New South Wales, the *Workplace Surveillance Act 2005* regulates and restricts the use of surveillance technologies in the place of one's employment.[15] Meanwhile, the *Surveillance Devices Act 2007* regulates the installation, use and maintenance of optical, listening or tracking devices by individuals and restricts their ability to observe, through these technologies, conversations and images to which they are not a party to.[16] A brief outline of both Acts is summarised below.

The *Workplace Surveillance Act 2005* repealed the previous *Workplace Video Surveillance Act 1998.* In doing so, the new Act broadened the definition of 'surveillance' from being merely about video surveillance, to also including computer surveillance (such as email monitoring) and tracking surveillance (through the use of GPS technologies).

---

[13] Carolyn Doyle & Mirko Bagaric, *Privacy Law in Australia,* The Federation Press 2005 at p 50.

[14] The Australian Privacy Charter (1995) 2*Privacy Law and Policy Reporter* 44.

[15] *Workplace Surveillance Act 2005* (NSW) ss 9 – 22. For a detailed analysis of the Act see Lenny Roth, *Workplace Surveillance,* NSW Parliamentary Library Research Service 2004.

[16] *Surveillance Devices Act 2007* (NSW) ss 7 – 14

The *Workplace Surveillance Act 2005* provides that an employer can only undertake surveillance of an employee provided that the employer has first notified the employee of the surveillance that will take place.[17] Further, the *Workplace Surveillance Act 2005* prohibits surveillance in certain circumstances (such as camera surveillance in change rooms)[18] and limits the ability to undertake covert surveillance to circumstances where a Magistrate has issued a covert surveillance authority for the purposes of establishing whether an employee is engaged in any unlawful activity.[19] Importantly, a Magistrate must consider whether covert surveillance of the employee or employees concerned might unduly intrude on their privacy or the privacy of any other person.[20]

The *Surveillance Devices Act 2007* replaces the *Listening Devices Act 1984* and 'is broader both in its application and effect'.[21] Like the *Workplace Surveillance Act 2005,* the *Surveillance Devices Act 2007* extends the application of surveillance to include data surveillance and tracking surveillance, placing general prohibitions on the use of these technologies unless consent is provided or for a 'lawful purpose'. Specifically, sections 7, 8, 9 and 10 of the Act respectively prohibit the use of listening devices, optical devices, tracking devices and data surveillance. Breaches of these provisions are criminal offences and can attract heavy penalties.

The Act prohibits a person from publishing or communicating to any other person, any record or a report of private conversations that came to their knowledge as a result of direct or indirect surveillance in contravention of the Act. To this end, the *Surveillance Devices Act 2007* seeks to limit the interference with the privacy of the affected individual by not only prohibiting covert surveillance of the individual but also seeking to limit the damage caused by prohibiting the dissemination of any information that was ascertained from the surveillance.

Much of the recent legislation passed has been influenced by increasing community concern about 'snoops' and 'peeping toms' using emerging technologies, such as camera phones, to take covert and improper photos of unwitting and unwilling parties. Although fear about 'peeping toms' is not new, technological advancement has made spying on people easier, and spreading the images or sounds that are captured even easier than that. Recent examples have been reported in the media where men have been caught taking inappropriate photos of women with their camera phones.[22]

But surveillance does not need to be so obvious. Merely surfing the Internet throws wide open the door to creative uses of surveillance. From the use of cookies that track a user's movements across the web, to spyware programs that surreptitiously collect information about a user's

[17] *Workplace Surveillance Act 2005* (NSW) ss 10

[18] *Workplace Surveillance Act 2005* (NSW) ss 15 –18

[19] *Workplace Surveillance Act 2005* (NSW) ss 23 – 35

[20] *Workplace Surveillance Act 2005* (NSW) s 26

[21] Sophie Dawson & Helen Gill, *Surveillance and the media: working within the confines of the new NSW Surveillance Devices Act,* (2008) 4(9) Priv LB at pp 110 – 115.

[22] Rick Wallace, *'Laws crack down on 'upskirt' snappers',* The Daily Telegraph, 28 July 2006.

browsing activities, to keystroke monitoring,[23] our increasing reliance on an electronic existence has meant that we invariably leave behind traceable, digital fingerprints.

While legislation seeks to regulate the use of surveillance technologies, one of the ongoing concerns is that the very nature of covert surveillance is that affected individuals are not aware that it is taking place. Every day, reams of personal data could be compiled and collated without any obvious indication to the affected person that this is taking place.

Some of the concerns about privacy-invasive technologies are discussed later.

3.2 Communications Privacy

Similarly related to surveillance privacy, communications privacy is about protecting the integrity of correspondence and the information contained in that correspondence. Threats to communications privacy have been addressed in the Surveillance Acts discussed above but prohibitions against interceptions are provided for in the *Telecommunications (Interception) Act 1979* (Cth).

Specifically, Part 13 of the *Telecommunications (Interception) Act 1979* (Cth) obliges carriers and carriage service providers to maintain the confidentiality of the contents or substance of communications carried through their systems. The Act prohibits the interception of communications over a telecommunications system. Communication is defined broadly to include, not just speech, but also texts, visual images, data and signals, along with any combination of these forms.[24] Interception is understood to mean listening to or recording communications that take place over a telecommunications system without the knowledge of the parties to the communication.[25] However, there are numerous exceptions to this rule. For example, the protection against interception does not apply to employees against their employers in the course of their employment.[26]

Meanwhile, Part 7B of the *Australian Postal Corporation Act 1989* (Cth) obliges postal carriers to adhere to strict conditions to maintain the integrity of mail being processed through the course of the post. The Act places strict limits on postal employees from opening and examining mail unless required to do so for security or quarantine reasons.[27] The Act also prohibits employees and former employees from using and disclosing information derived from the mail unless in certain, specifically prescribed circumstances, such as under the authority of a warrant.[28]

3.3 Bodily Privacy

[23] Such as the Trojan horse 'Zlob Trojan'.

[24] *Telecommunications Act 1997* (Cth) s 7

[25] Carolyn Doyle & Mirko Bagaric, *Privacy Law in Australia,* The Federation Press 2005 at p 141.

[26] Ibid at p 142.

[27] *Australian Postal Corporation Act 1989* (Cth), ss 90M – 90X

[28] *Australian Postal Corporation Act 1989* (Cth), ss 90G – 90LF

Bodily privacy is about ensuring that the physical body is not subjected to arbitrary interferences, either by the State (such as unwarranted searches by police) or by other individuals (such as assault, battery and false imprisonment). Bodily privacy is fundamentally about respecting the integrity of the physical self and protecting the 'personal space' that immediately surrounds the body from unsolicited encroachment.

Whether or not there is a right to 'bodily privacy' is the subject of much discussion. For the most part, an interference with ones' bodily integrity has not been historically regarded as an invasion of privacy per se, but has been examined through the prism of other torts, such as nuisance, trespass or false imprisonment. Depending on the severity of the invasion, the interference with one's bodily integrity may be criminal in nature, for example in instances of assault and battery.

Bodily privacy is not also about limiting the ability to take samples and extract information from the body. A common example is that motorists will often be required to submit to breathalysers that monitor blood alcohol levels or face arrest for failure to cooperate. Technological advancement has meant that retina scans, DNA tests and even psychometric testing are all possible.

While the collation of the data obtained form collections of this nature is covered under laws regulating information privacy, undergoing these scans or tests may be considered an affront to bodily privacy and, for some individuals, a deeply personal and violating experience.

3.4 Territorial Privacy

Territorial privacy is about allowing individuals a right to a private sphere in which to conduct their personal affairs without interference or surveillance and a degree of control over access to one's private domain. This right applies not only in a person's home but also to varying degrees, in the workplace, the use of recreational facilities and public places.[29] Privacy is also a latent consideration when spatial concerns are factored into planning laws, or when limitations are placed on real estate agent inspections in residential tenancy laws.

Violations of territorial privacy may often result from a breach of a (non-privacy related) Act, can be examined through the tort of trespass or, increasingly, may be examined through the tort of privacy at the common law.

3.5 Personal Information Privacy

Personal information privacy has been defined as

> the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. [30]

Personal information is fundamentally about the control of data that identifies and defines individuals, the individual having a say *who* has access to the information about them and *why*,

[29] See cl. 8 of the *Australian Privacy Charter* at www.privacy.org.au accessed 21 May 2008.

[30] Allan F. Westin, *Privacy and Freedom,* Atheneum New York 1967 at p 7.

as well as how the information is gathered, stored and used.[31]

Understanding what is considered personal information is inexact. Personal information has two requisite parts, that which is *personal* i.e. that which identifies an individual, and that which is *information* i.e. facts or opinions about the individual that gives meaning and character to the individual's identity.

Legally, personal information itself has been defined as:

> information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.[32]

The sweeping nature of this definition captures a wide amount of information. Personal information can therefore mean to include such data as a name and may include addresses, dates of birth and occupations as well as medical conditions and financial details. In fact, any article of information or permutation of bits of information about an individual can be deemed 'personal information' if the information gives rise to an identity that is 'apparent' or can 'reasonably be ascertained'.

Often, information can only be deemed as *personal* after consolidating disparate pieces of data that, if left isolated, would fail to identify the individual. For example, quarantining information about a person's date of birth, occupation and residence would be meaningless but once aggregated, may accurately reveal the identity of the person. In this regard, 'personal information' is almost entirely context-sensitive and relative to other people.

In Australia, legislation has been introduced at the Federal level and in some States that regulates personal information. At the Federal Level, the *Privacy Act 1988* (Cth) obliges most Commonwealth Government agencies, together with some parts of the private sector, to adhere to a set of standards regarding the way personal information is collected, disclosed and used, as well as providing for access and amendment rights to individuals. Meanwhile at the State level, the *Privacy and Personal Information Protection Act 1998* (NSW) includes the Information Protection Principles that provides for similar obligations for NSW State Government agencies.

In addition, the *Health Records and Information Privacy Act 2002* (NSW) governs the handling of health information by both public sector agencies and private organisations. The Act includes the 15 Health Privacy Principles that broadly cover the collection, storage, use, access and disclosure of health information. The Act came into effect on 1 September 2004.

---

[31] Gareth Griffith, *Privacy Law Reform: Issues and Developments,* NSW Parliamentary Library Research Service 1998 at p 8.

[32] *Privacy Act 1988 (Cth)* s 6, *Privacy and Personal Information Protection Act 1998 (NSW)* s 4.

Regulation about information privacy is the most comprehensive and regulated of all the sub-categories of privacy that have been identified. Across the jurisdictions, laws regarding information privacy have been largely derived from international precedent.

4 INTERNATIONAL OBLIGATIONS

The development of privacy law in Australia is largely a result of directly importing international human rights instruments into domestic law by ratification. As various international human rights instruments have enumerated privacy, privacy was therefore anchored in Australia's legal tradition through its obligations under international law.[33]

The *International Covenant on Civil and Political Rights* (the 'ICCPR') was ratified by Australia on 13 August 1980 and entered into force on 13 November 1980. Article 17 of the ICCPR provides:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour or reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.

The ratification of the ICCPR was the first time a right to privacy was introduced into Australia with some legal recognition, even though it was not directly incorporated into a Bill of Rights or other equivalent statute.

Article 12 of the *Universal Declaration of Human Rights* is an almost identical provision to article 17 of the ICCPR and article 16 of the *Convention of the Rights of the Child* is likewise substantially similar, but with specific reference to children.

In 1991, Australia acceded to the First Optional Protocol to the ICCPR that gives an applicant certain rights to bring a case for infringement of one of the rights enumerated under the ICCPR to the United National Human Rights Committee. However, an applicant may only do so in certain situations and where all available domestic remedies have been exhausted.[34]

In addition to the ICCPR, privacy rights were given further depth and definition with the development of the Organisation for Economic Cooperation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* These Guidelines provide that OECD member countries should adopt 'Basic Principles of National Application' that provides the way personal information about an individual is collected, used, disclosed and stored as well as providing a general right of access by individuals to their personal information and a right to have the information amended.[35] These guidelines were developed to strike an

[33] There has been lengthy discussion about whether privacy is a 'human right' or an 'interest', for example see Carolyn Doyle & Mirko Bagaric, *Privacy Law in Australia,* The Federation Press 2005.

[34] *Optional Protocol to the International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, entered into force in Australia 25 September 1991, http://www2.ohchr.org/english/bodies/ratification/5.htm accessed on 29 April 2008.

[35] The OECD Guidelines are available at http://www.oecd.org.

appropriate balance between ensuring privacy is protected and facilitating the free flow of information.[36]

The preamble to the *Privacy Act* 1988 (Cth) ('Privacy Act') specifically refers to both the ICCPR and the OECD Guidelines and the Act itself gives effect to the OECD Guidelines and partial effect to the ICCPR.[37]

There are some significant differences between the ICCPR and the OECD Guidelines, the most notable of which is that the ICCPR has treaty status and is expressed in broad, abstract language. The OECD Guidelines, meanwhile, do not have treaty status and are expressed in specific terms.[38] Also, the OECD Guidelines relate almost exclusively to 'information privacy' whereas the ICCPR also refers to privacy generally.

The last International instrument that had some bearing on the development of information privacy law in Australia was the European Union's (EU) *Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (EU Data Protection Directive 95/46/EC). This directive was issued in 1995 to ensure that the citizens of the EU do not lose privacy protections when their personal data is transferred outside of EU member countries. Specifically, article 25 of the EU Directive restricts disclosures of personal data from EU states to external jurisdictions which did not have an adequate level of legal protection for such data. This measure increased pressure for those jurisdictions that did not have adequate privacy protections to bring their privacy laws into line with evolving international standards. The EU's Directive had some indirect influence on the broadening of Australia's privacy law to cover parts of the private sector and the State Government sector.[39]

5 PRIVACY LAW IN AUSTRALIA

The Australian Constitution does not provide a conclusive view about which jurisdiction, State / Territory or Federal, is responsible for privacy regulation. As such, each State and Territory, together with the Commonwealth, is able to enact relevant legislation.

As such, privacy law in Australia has been established by several statute-based regulatory regimes that handle 'information privacy'. In New South Wales and at the Commonwealth level, there are separate Acts concerned with information privacy. Each of the other States and the Northern Territory have either legislative or administrative arrangements in place with respect to the regulation of personal information management.

The principal federal statute that handles information privacy is the *Privacy Act 1988* (Cth) ('Privacy Act'). The Privacy Act provides for a Commission to regulate the way in which those organisations within its remit handle personal information, rather than providing a tort of privacy

---

[36] Australian Law Reform Commission, *Review of Australian Privacy Law – Discussion Paper 72,* September 2007 at p 545.

[37] Office of the Privacy Commissioner, The operation of the Privacy Act annual report: 1 July 2006 – 30 June 2007 at p 81.

[38] Margaret Jackson, Hughes on Data Protection in Australia, Lawbook Co 2001 at p 25.

[39] *International Privacy Standards,* Privacy Victoria, 30 June 2003.

generating a right to a cause of action at civil law.

The Privacy Act was initiated in 1988 in the aftermath of the Hawke Government's attempts to introduce an 'Australia Card'. In 1985, the Hawke Government floated the possibility of a national identification scheme. The intention of the project was that the Government would issue a card – dubbed the 'Australia Card' – to every individual for the purposes of combating tax evasion, welfare fraud and illegal immigration.[40]

The elements of the scheme were that everyone would receive a unique identifier encoded in a card that would be linked to a central register. This card would be use to access Government services and Government agencies would compel production of the card. As a result of heated public debate, opinion polls showing increasing disfavour of such a card and rejection of the Card by the Senate (which precipitated a double dissolution election), the Hawke Government dropped the proposal.[41]

The fallout from the Australia Card debate together with international trends and obligations prompted the Hawke Government to enact privacy legislation and establish the Office of the Privacy Commissioner.

Initially, the Privacy Act provided obligations only for Commonwealth Government departments and agencies. These obligations are set out in the Information Privacy Principles (IPPs) in section 14 of the Privacy Act. The IPPs set out the requirements for the manner and method in which Commonwealth public sector agencies collect, use, disclose and store personal information. The IPPs also set out requirements to allow individuals to have access to their personal information and require agencies to set out policies on how they handle personal information. Separate to the IPPs, the Privacy Act also regulates the use of Tax File Numbers (TFNs).

In 1990, coverage of the Privacy Act was extended to include consumer credit reporting. In particular, the Act included specific provisions for consumer credit providers and consumer credit reporting agencies on the nature of credit reports and overall creditworthiness of individuals.

In 2001, coverage of the Privacy Act was extended to include parts of the private sector, including businesses with an annual turnover of more than $3 million, health service providers, businesses that trade in personal information for a benefit, service or advantage, subsidiary groups of larger organisations and small businesses that opt into coverage of the Act or recognised code. The National Privacy Principles (NPPs), which are distinct from the IPPs, were included in Schedule 3 of the Privacy Act to apply to those parts of the private sector covered by the Act. The NPPs draw on the IPPs but expand on them and include several additional provisions. These additional provisions reflect changes in the privacy landscape. They prohibit the use of Government identifiers as a de facto identification system in the private sector, allow for anonymity when dealing with organisations in certain situations, regulate the use of personal

[40] Graham Greenleaf, *The Australia Card: Towards a National Surveillance System* at http://austlii.edu.au/itlaw/articles/GGozcard.html, accessed 1 May 2008.

[41] Roger Clarke, *Just Another Piece of Plastic in your Wallet: The 'Australia Card' Scheme* at http://www.anu.edu.au/people/Roger.Clarke/DV/OzCard.html, accessed 1 May 2008.

data being transferred offshore and provide additional protections for information deemed 'sensitive'.

Administration of the *Privacy Act 1988* (Cth) is the responsibility of the Office of the Privacy Commissioner. It has responsibilities for handling complaints and investigating alleged breaches of the *Privacy Act 1988* (Cth) by Commonwealth Government agencies and those private sector organisations that fall under its jurisdiction.

Although a Federal Act with responsibilities at the Federal level, the *Privacy Act 1988* is applicable in New South Wales through its coverage of some private sector organisations. During debates in New South Wales on whether or not to extend coverage of the *Privacy and Personal Information Protection Act 1998* to cover the private sector, one of the arguments in favour of extending the application was that the Commonwealth Government had, until that time, not enacted privacy legislation that covered the private sector. It was decided that a uniform and holistic approach was more appropriate and the issue of private sector coverage was informally referred to the Commonwealth Government.[42] Amendments to the *Privacy Act 1998* in 2001 partially covered the field with respect to the private sector.

6 THE HISTORY OF PRIVACY LAW IN NSW

In 1972, the Standing Committee of Attorneys-General commissioned a report on privacy. In 1973, the Morrison Report was delivered to the then Justice Minister, the Hon. J Maddison, in which it recommended that there should be a:

> general legislative provision for the protection of privacy of the individual against threats existing and foreseeable.[43]

New South Wales was then the first State to enact a version of a privacy regime with the passing of the *Privacy Committee Act 1975* (NSW). This Committee was established to provide for a 'privacy ombudsman'. The Privacy Committee had a largely advisory and investigatory role in the management and monitoring of privacy issues in NSW and did not have any effective powers to enforce privacy principles in either the public or private sectors.[44] Its powers were largely limited to undertaking research into matters that affected the privacy of an individual, investigating complaints, undertaking educational tasks and drafting reports and recommendations that related to possible legislative and administrative initiatives to better protect the privacy of individuals. The Committee also had the power to compel production of information or documents, with the failure to comply deemed a criminal offence. Throughout the 1980s, the Committee agitated for legislative reform and the establishment a principle-based privacy code.[45]

---

[42] The Hon. J. W. Shaw in NSWPD, 17 September 1998 at p 7601.

[43] Privacy NSW, *Submission to the Review of the Privacy and Personal Information Protection Act 1998,* 24 June 2004 at p 14.

[44] Vicki Mullen, *The individuals right to privacy: Protection of personal information in NSW*, NSW Parliamentary Library, Briefing Paper No 14/95 at pp 8 – 9.

[45] Margaret Jackson, *Hughes on Data Protection in Australia,* Lawbook Co, 2001 at pp 170 – 172.

In 1991, Andrew Tink MP introduced a private member's Bill, the *Data Protection Bill*, which provided for information privacy protections in both the public and private sectors. Debate on the legislation was deferred until after the release of an Independent Commission Against Corruption ('ICAC') enquiry that was in the process of drafting a report into the unauthorised trade of personal information amongst Government agencies.

In 1992, this ICAC investigation uncovered a network of Government officers selling to other Government agency officers the personal information of individuals that they had access to. This network was dubbed the 'Information Exchange Club'. In its report, ICAC found that:

> an uncontrolled system of exchange of information developed, in which access to information depended on the unofficial private contacts a person had.
>
> Unauthorised dissemination of confidential Government information resulted. The Information Exchange Club became a source of information, both for those who sought it for what they regarded as a legitimate purpose, and for others who wanted it for re-sale.[46]

ICAC also uncovered a trade in information from Government agencies to insurance companies and financial institutions. Often, the trade resulted in a cash payment. In light of the flourishing trade in personal information, ICAC supported moves by the Government of the day to pass data protection legislation that protected personal information held by State Government agencies from misuse[47] and addressed the inadequacies in the legislative arrangements of the time in dealing with the abuse of personal information.

Specifically, ICAC recommended that the development of a privacy regime was a necessary precondition to rebuilding public trust in Government:

> efficient data security and protection, and ... a consistent and effective body of law to control the handling of confidential government information…are necessary to overcome the corrupt trade that has developed.[48]

ICAC also recommended that access to protected information be strictly limited, that unauthorised dealing in Government information be rendered a criminal offence and that attempts should be made to have legislation adopted throughout the Commonwealth that is at least consistent, if not uniform.

The Privacy Committee added weight to ICAC's recommendation, noting that:

> Personal information provided in good faith (and, frequently, under legal compulsion) by the citizens of New South Wales is being bartered and sold on a breathtaking scale. Our

[46] Independent Commission Against Corruption, *Report on the unauthorised release of Government information: Volume I,* August 1992 at pp 13 – 14.

[47] Independent Commission Against Corruption, *Report on the unauthorised release of Government information: Volume I,* August 1992 at p 117.

[48] Independent Commission Against Corruption, *Report on the unauthorised release of Government information: Volume I,* August 1992 at p 120.

privacy is being sold and the proceeds of the sale are lining the pockets of the corrupt.[49]

In 1994, the *Privacy and Data Protection Bill 1994*, amended from the initial Bill, was introduced by the then Attorney General, the Hon. JP Hannaford MLC. The Bill was referred to a Select Committee of the Legislative Council for review. However, before the Committee was able to table a report, the Bill lapsed and there was a change of Government following the March 1995 State election.

The new Attorney- General, the Hon. JW Shaw QC, MLC, introduced a revamped privacy bill – the *Privacy and Personal Information Protection Bill 1988* – into Parliament. The Attorney-General noted the significant influence the ICAC report had in creating a more comprehensive privacy regime in his Second Reading Speech to Parliament.[50]

The Bill introduced Information Protection Principles to the public sector in New South Wales, preferring to leave coverage of the private sector until a uniform approach on a national basis could be devised.[51]

There was also much debate about whether State Owned Corporations should be included in the Act. Initially, they were excluded but the Opposition moved an amendment in the Legislative Council to include them. This amendment was then overturned in the Legislative Assembly due to the concern that State Owned Corporations, which competed for business in the private sector, would be put at a 'competitive disadvantage' if they had to adhere to obligations not required of their counterparts in the private sector.[52]

After much debate and amendment, the Bill was enacted on 1 December 1998.

7 THE PRIVACY AND PERSONAL INFORMATION PROTECTION ACT 1988

The *Privacy and Personal Information Protection 1988* (NSW) is the primary statute that pertain to personal information privacy. The Act applies to New South Wales public sector agencies, including local government authorities, the teaching service and NSW Police Force, although there are also numerous exemptions, specifically for law enforcement agencies and state-owned corporations.[53] Health information in the New South Wales public sector is separately handled by the *Health Records and Information Privacy Act 1988* (NSW).

7.1 The Information Protection Principles

The Privacy and Personal Information Protection Act contains the Information Protection

[49] The Privacy Committee of New South Wales, *Privacy and data protection in New South Wales, a proposal for legislation,* Submission to the Independent Commission Against Corruption, No 63 June 1991 at p. 1

[50] The Hon. J.W. Shaw in NSWPD, 17 September 1998 at p 7600.

[51] Ibid at p 7601.

[52] The Hon. Paul Whelan MP in NSWPD, 18 November 2008 at p 10276.

[53] *Privacy and Personal Information Protection Act* 1998 (NSW) s 3

Principles. As with most legislation concerning data protection, the principles are based on the 1980 OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data and as such are structurally similar (but contents-wise, different) to the equivalent Information Privacy Principles in the *Privacy Act 1988* (Cth).

The principles of the Act are set out in sections 8 to 19 and broadly deal with the following:

8. *Collection of personal information for lawful purposes*: An agency must not collect personal information unless it is for a lawful purpose directly related to the functions of the agency and the information is reasonably necessary for that purpose.

9. *Collection of personal information directly from the individual:* An agency must collect information about an individual directly from the individual concerned unless the individual authorises the agency to collect from other sources or, in the case individuals under 16 years of age, the information has been provided by a parent or guardian.

10. *Requirements when collecting personal information:* In the process of collecting personal information, an agency needs to ensure that it gives notice to the individual that information is being collected, make the individual aware of the purpose of the collection, to whom the information will be forwarded to, whether the collection of information is required or authorised by law, any access and correction rights that may apply, and the agency's contact details.

11. *Other requirements relating to collection of personal information:* In the process of collecting personal information, an agency needs to ensure that the information collected is relevant to its purpose, is accurate and does not unreasonably intrude into the personal affairs of the individual.

12. *Retention and security of personal information:* An agency must not keep information for longer than is necessary for the purposes for which it may be lawfully used, the information must be stored securely, must be disposed of securely and reasonable steps must be taken to ensure the information is not used or disclosed without authorisation.

13. *Information about personal information held by agencies:* An agency must take reasonable steps to enable an individual to ascertain whether the agency holds information about them, the nature of the information that the agency holds, the purpose for which the information is used, and how the individual can access the information.

14. *Access to personal information held by agencies:* An agency must provide individuals with access to their personal information, upon request by the individual.

15. *Alteration of personal information:* An agency must permit an individual to check the accuracy and relevance of information and, if information is amended, notify the individual of the amendment. If the agency is not prepared to amend the record, the agency must allow the individual to provide a statement on the record about the amendment sought.

16. *Agency must check accuracy of personal information before use*: An agency must take reasonable steps to ensure that the information it holds about an individual is accurate,

complete and up to date, before using the information.

17. *Limits on use of personal information:* An agency must not use personal information for a use other than the use for which it was collected, unless the individual to whom the information relates to consents to the use, or the use is directly related to the use for which it was collected, or the use of the information for the other purpose is necessary to prevent or lessen serious or imminent harm.

18. *Limits on disclosure of personal information:* An agency must not disclose personal information unless than disclosure is directly related to the purpose for which the information was collected, or the individual about who it relates to is reasonably likely to be aware that the information would be disclosed, or the information needs to be disclosed because of a serious and imminent threat to an individual.

19. *Special restrictions on disclosure of personal information:* An agency must not disclose sensitive information about an individual – such as ethnic origin, political opinions, religious beliefs, sexual orientation etc – unless it does so to prevent a serious and imminent threat to the life of an individual. An agency is also prohibited from transferring data to jurisdictions that do not have relevant a privacy law or privacy code.

Section 8 – 11 do not apply to personal information collected by an agency before the commencement of the Act although the remaining principles apply to personal information collected by agencies regardless if the information was collected before or after the commencement of the Act.

The principles frequently refer to 'personal information' and the primary purpose of the Act is to protect the integrity of 'personal information'. Personal information is defined in section 4 of the Act as:

> Information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.[54]

The Act expressly provides that personal information can also include biometric data, such as fingerprints, retina prints, body samples or genetic characteristics.[55] However, health information is expressly excluded from the definition of personal information as it is separately dealt with by the *Health Information and Privacy Records Act 1992*.[56]

[54] *Privacy and Personal Information Protection Act 1988* (NSW) s 4(1)

[55] *Privacy and Personal Information Protection Act 1988* (NSW) s 4(2)

[56] *Privacy and Personal Information Protection Act 1988* (NSW) s 4A

7.2 Exemptions

The definition of personal information also contains a comprehensive list of exemptions. For example, personal information does not include information relating to an individual who has been deceased for more than 30 years[57] and information about an individual that is contained in a publicly available record.[58]

The extensive, although non-exhaustive, list of exclusions also include:

- information about a witness who is included in a witness protection program under the *Witness Protection Act 1995*;
- information about an individual arising out of a warrant under the *Telecommunications (Interception) Act 1979 of the Commonwealth;*
- information about an individual arising out of a protected disclosure in accordance with the *Protected Disclosures Act 1994;*
- information about an individual arising out of, or in connection with, a law enforcement operation in accordance with the *Law Enforcement (Controlled Operations) Act 1997;* and
- Information arising out of a Royal Commission or Special Commission of Inquiry.

The list is long and doubts have been raised as to whether there are strong enough reasons to warrant so many exclusions.[59]

There are numerous other provisions that provide for specific agencies to be exempt from some, or all of the principles of the Act. For example, ICAC and the NSW Police Service are specifically exempted from adhering to part of the Information Protection Principles of the Act except in relation to their administrate functions.[60]

Meanwhile sections 24 and 25 of the Act provide for partial exemptions for law enforcement and investigatory agencies in certain circumstances. For example, under section 23(4) of the Act, a public sector agency is not required to comply with the principle that limits the use of personal information if the use of the information concerned a purpose other than the purpose for which it was collected, is reasonably necessary for law enforcement purposes or for the protection of the public revenue. The creation of partial exemptions from the principles for some agencies in

[57] *Privacy and Personal Information Protection Act 1988* (NSW) s 4(3)(a). Note the difference with the s 6 of the *Privacy Act 1988* (Cth) that defines that personal information only applies to 'natural persons', that is, individuals that are living.

[58] *Privacy and Personal Information Protection Act 1988* (NSW) s 4(3)(b)

[59] Moira Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State,* LexisNexis Butterworths 2005 at p 73.

[60] *Privacy and Personal Information Protection Act 1998* (NSW) s 27

certain circumstances has attracted criticism for its confusing nature and the difficulty in applying the law consistently. [61]

Section 5 of the Act also provides that the operation of the *Privacy and Personal Information Protection Act 1998* does not affect the operation of the *Freedom of Information Act 1989* while section 20(5) provides that certain protection principles (regarding *Information about personal information held by agencies, Access to personal information held by agencies* and *Alteration of personal information)* do not affect any condition or limitation arising out of the *Freedom of Information Act 1989.*

7.3 Privacy Codes of Practice

The Act also allows for a Government agency to modify the IPPs through the application of a code of practice. The Privacy Commissioner or a public sector agency may initiate the preparation of a draft privacy code which may modify the application of the IPPs to a public sector agency or may exempt the agency, or class of agency, from compliance with an IPP.[62] The Privacy Commissioner may submit the draft code to the Minister along with any submissions that the Privacy Commissioner thinks appropriate.[63] The code takes effect by an order of the Minister published in the Gazette.[64]

7.4 Management Plans

Each public sector agency was required to devise a privacy management plan and lodge the plan with the Privacy Commissioner by 1 July 2000. Privacy management plans are strategic documents where the public sector agency describes the measures in place to ensure compliance with the information protection principles and the public register provisions of the Act. The plans may be amended, as the agency deems appropriate.

7.5 The Commissioner and the Complaints Process

Section 36 of the Act provides a lengthy list of functions conferred onto the Privacy Commissioner.

A list of some of the functions is as follows:

- to promote the adoption of, and monitor compliance with, the information protection principles.[65]

- to provide assistance to public sector agencies in adopting and complying with the

[61] Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998,* June 2004 at p 32.

[62] *Privacy and Personal Information Protection Act 1998* (NSW) ss 30(1) and 30(2)(a) – (c)

[63] *Privacy and Personal Information Protection Act 1998* (NSW) ss 31(1) and 31(3)

[64] *Privacy and Personal Information Protection Act 1998* (NSW) s 31(5)

[65] *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(a)

information protection principles and privacy codes of practice.[66]

- to conduct research, and collect and collate information, about any matter relating to the protection of personal information and the privacy of individuals.[67]

- to conduct education programs, and to disseminate information, for the purpose of promoting the protection of the privacy of individuals.[68]

- to prepare and publish reports and recommendations about any matter (including developments in technology) that concerns the need for, or the desirability of, legislative, administrative or other action in the interest of the privacy of individuals.[69]

Another one of the functions of the Privacy Commissioner is to receive complaints about the violation or interference with an individual's privacy and, where appropriate, undertake preliminary assessment and investigations into the matter with a view to conciliating the complaint between the disputing parties.[70]

Generally, a privacy complaint must be made within six months of the affected individual being made aware of the matter that is the subject of the complaint. The Privacy Commissioner may make preliminary assessments of the subject of the complaint for the purpose of deciding whether to deal with the complaint. Regard may be given to whether the complaint is frivolous, vexatious, lacking in substance, trivial or where there are other remedies that may be more appropriate in the circumstances.

7.6 Internal Reviews

The Commissioner may assist a named agency in conducting an internal review. Section 53(1) of the Act provides that an applicant who is aggrieved by the conduct of a public sector agency is entitled to a review of that conduct. After completion of the internal review, the agency is able to do any number of things, including, take no further action, issuing an apology, remedial action such as monetary compensation, an undertaking that the offensive conduct will not recur and implementing administrative arrangements to ensure the offensive conduct will not recur.

The agency must notify the Privacy Commissioner that a request for an internal review has been received and keep the Privacy Commissioner informed of the progress and findings of the review.

If the applicant is dissatisfied with the findings of the review, or dissatisfied with the conduct of the agency in the course of its review, then the applicant can appeal to the Administrative Review Tribunal. The Tribunal can issue orders that require an agency to refrain from certain

---

[66] *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(d)

[67] *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(f)

[68] *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(i)

[69] *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(j)

[70] *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(k)-(l)

conduct, perform an obligation and take steps to remedy the loss or damage caused to the applicant. In circumstances where the conduct of the agency has resulted in financial loss or physical or psychological harm, the Tribunal can award damages up to $40,000.

7.7 Offences under the Act

The Act also criminalises corrupt disclosures of personal information. Section 62 and 63 of the Act provide that a person who intentionally discloses personal information outside of the course of their duties, or attempts to induce a bribe for the supply of personal information or solicits a bribe in exchange for personal information, can be deemed guilty of a criminal offence that carries up to two years imprisonment. Section 62(3) does however provide an exception for whistleblowers, which ensures that public servants are not prohibited from disclosing personal information in circumstances that are in accordance with the *Protected Disclosures Act 1994.* The Act also provides for offences relating to the wilful obstruction of the Privacy Commissioner in the exercise of his or her functions and making false or misleading statements to the Privacy Commissioner.[71]

7.8 The Health Records and Information Privacy Act 2002

In December 2000, the NSW Ministerial Advisory Committee on Privacy and Health Information released its report *Panacea or Placebo?* in which it recommended that 'the system of linked electronic health records be governed by a separate and specific piece of State legislation'[72]. Subsequently, the *Health Records and Information Privacy Act 2002* (NSW) was enacted which includes the Health Privacy Principles (HPPs). These principles were modelled on the NPPs of the *Privacy Act 1988* (Cth) and designed to build on existing obligations required of health service providers.[73] While the *Privacy Act 1988* (Cth) covers private sector health service providers and the *Privacy and Personal Information Protection Act 1998* (NSW) covers State public sector health service providers, the *Health Records and Information Privacy Act 2002* (NSW) provides an additional layer of obligations on health service providers at both the private and State public level.[74]

The HPPs apply to all organisations that hold health information defined as information or an opinion about a person's physical or mental health or a disability of an individual.[75] The HPPs do not apply to information held by individuals in relation to their household affairs, news media outlets, group practices or certain statutory authorities.[76] Many of the HPPs are mere restatements of existing privacy principles in both the State IPPs and the Federal NPPs. However, the Act contains additional provisions to the HPPs that are more prescriptive and assist in the operation of the HPPs. For example, while section 14 of the *Privacy and Personal*

[71] *Privacy and Personal Information Protection Act 1998* (NSW) s 68

[72] Gareth Griffith, *Information Privacy and Health Records,* NSW Parliamentary Library Research Service, April 2002 at p 30.

[73] Ibid at p 31.

[74] *Health Records and Information Privacy Act 2002* (NSW), s 11

[75] *Health Records and Information Privacy Act 2002* (NSW), s 6

[76] *Health Records and Information Privacy Act 2002* (NSW), ss 14 – 17

Information Protection Act 1998 (NSW) and NPP 6 in the *Privacy Act 1988* (Cth) respectively requires an agency or organisation to provide access to health information on request by the individual concerned, neither principle stipulates a deadline for providing access. The *Health Records and Information Privacy Act 2002* (NSW), meanwhile, provides for a general right of access at HPP 7 but, additionally, stipulates a limit of 45 days for health service providers to allow access or a statement explaining the reasons for refusal to allow access.[77] To this end, the *Health Records and Information Act 2002* (NSW) provides more guidance for compliance with the principles of the *Health Records and Information Act 2002* (NSW) than either the *Privacy Act 1988* (Cth) or the *Privacy and Personal Information Protection Act 1998* (NSW). Complaints about alleged breaches of the *Health Records and Information Act 2002* (NSW) are the responsibility of the Privacy Commissioner.

The HPPs also include an additional principle regarding the linkage of health records. This principle provides that, generally, an organisation must not include the health information of an individual on a health records linkage system unless the individual has the expressly consented to the information being included on such a system.[78] This principle is notably absent from the State IPPs as well as both the Federal IPPs and NPPs.

8 PRIVACY AT THE COMMON LAW

While there is a suite of developed legislation that, in some way, touches on privacy law, the development of privacy at the common law is nascent.

In Australia, historically, the common law has largely refused to recognise an actionable right to privacy.[79] However, the question of whether privacy exists as a common law right, or should exist as a right, has been the subject of judicial consideration in a number of cases.

For six decades, the law on privacy was primarily drawn from the High Court's judgement in *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* in which Latham CJ said in considering the arguments raised in favour of finding a tort of privacy:

> However desirable some limitation upon the invasions of privacy might be, no authority was cited which shows that any general right of privacy exists.[80]

The position of the common law on the question of privacy remained unaltered and largely uncontested, and the experience for the ensuing six decades was that the position of the Court in *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* was settled law.

Musings about the development of a tort of privacy developed in the intermittent years. In *Church of Scientology Inc v Woodward*, Murphy J identified 'an unjustified invasion of privacy'

---

[77] *Health Records and Information Privacy Act 2002* (NSW), s 27

[78] *Health Records and Information Privacy Act 2002* (NSW), HPP 15

[79] See Carolyn Doyle & Mirko Bagaric, *Privacy Law in Australia,* The Federation Press 2005 at p 59.

[80] *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor ('Victoria Park Racing')* (1937) 58 CLR, 414

as a 'developing tort'[81]but did not elaborate on or progress the thought.

The issue was properly reignited in the recent case of *Australian Broadcasting Corporation v Lenah Meats Pty Ltd.*

In this case, Lenah Game Meats, the respondent, was a processor and supplier of possum meat. Individuals unknown to the respondent broke into the factory premises and covertly filmed the stunning and killing of possums for the production of its meat. The film of the incident was then passed on to the applicants, Australian Broadcasting Corporation ('ABC'). Lenah Game Meats then sought an interim injunction for the broadcasting of the film citing, *inter alia*, a right to privacy.

In considering the facts, Gleeson CJ noted:

> The respondent invited this Court to depart from old authority, declare that Australian law now recognises a tort of invasion of privacy; hold that it is available to be relied upon by corporations as well as individuals; and conclude that this is the missing cause of action for which everyone in the case has so far been searching.[82]

Despite refusing to recognise a tort of privacy in the circumstances of the case before the Court, Gleeson CJ did not close the door to recognising a tort of privacy all together. Specific to his concerns in *Lenah Game Meats* was that the applicant, a company, was asking for a recognition of its corporate privacy, noting that:

> Lenah's reliance upon an emergent tort of invasion of privacy is misplaced. Whatever development may take place in that field will be to the benefit of natural, not artificial, persons.[83]

Gleeson CJ continued:

> Nothing said in these reasons should be understood as foreclosing any such debate or as indicating any particular outcome. Nor, as already has been pointed out, should the decision in *Victoria Park*.[84]

The Court emphasised that its decision not to recognise a right of privacy for Lenah Game Meat's should not be interpreted as the Court precluding the existence of such a right, for natural persons, in future cases.[85]

---

[81] *Church of Scientology Inc v Woodward* (1982) 154 CLR 25, [13]

[82] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd ('Lenah Game Meats')* (2001) 208 CLR 199, [38]

[83] *Lenah Game Meats* (2001) 208 CLR 199, [132]

[84] *Lenah Game Meats* (2001) 208 CLR 199, [132]

[85] See Ken McKinnon, *'Privacy and the Press'*, Speech to the Commonwealth Press Union Conference on 25 February 2005 at http://www.presscouncil.org.au/pcsite/fop/cpu.html, accessed 30 April 2008.

Meanwhile, Callinan J compared the decision of the Court in *Lenah Game Meats* with that of *Victoria Park Racing*, noting that the decision of the Court in *Victoria Park Racing* was by a 'narrow majority'[86] and had 'the appearance of an anachronism'.[87] In *dicta*, Callinan J advised:

> It seems to me that, having regard to current conditions in this country, and developments of the law in other common law jurisdictions, the time is ripe for consideration whether a tort of invasion of privacy should be recognised in this country… [88]

The door for an actionable right of privacy in Australia was left ajar, examined further in the case of *Grosse v Purvis*.

In *Grosse v Purvis*, the plaintiff alleged that she had suffered psychological harm as a result of the defendant persistently harassing her. The plaintiff alleged that the defendant had loitered around her residence and workplace, had trespassed on her residential premises and had made nuisance phone calls.

In the case, Senior Judge Skoien noted Gleeson CJ's view in *Lenah Game Meats* that the decision in *Victoria Park Racing* presented 'no bar to the existence of a common law right to privacy'[89] and then proceeded to take, what in his Honour's words was, 'a bold step'[90] and 'as it seems, the first step in this country'[91] to unequivocally recognise an actionable right of privacy.

In identifying this right of privacy, his Honour then enumerated a four-pronged test detailing each of the essential elements of the new tort. They included:

(a) a willed act by the defendant,

(b) which intrudes upon the privacy or seclusion of the plaintiff,

(c) in a manner which would be considered highly offensive to a reasonable person of ordinary sensibilities, and

(d) which causes the plaintiff detriment in the form of mental, psychological, emotional harm or distress or which prevents or hinders the plaintiff from doing an act which s/he is lawfully entitled to do.[92]

His Honour found that each element of the test was satisfied by the plaintiff in *Grosse v Purvis* and subsequently awarded damages to the plaintiff totalling $178,000, including $20,000 in

[86] *Lenah Game Meats* (2001) 208 CLR 199, [316]

[87] *Lenah Game Meats* (2001) 208 CLR 199, [318]

[88] *Lenah Game Meats* (2001) 208 CLR 199, [335]

[89] *Grosse v Purvis* [2003] QDC 151, [428]

[90] *Grosse v Purvis* [2003] QDC 151, [442]

[91] *Grosse v Purvis* [2003] QDC 151, [442]

[92] *Grosse v Purvis* [2003] QDC 151, [444]

exemplary damages.[93]

A second noteworthy case in the development of the tort of privacy is *Jane Doe v Australian Broadcasting Corporation.* In this case, the defendant – a media broadcaster – published information that identified the victim of a sexual crime.

In her judgement, Judge Hampel acknowledged the existence of an actionable right of privacy, referring to the essential elements of the tort enumerated in *Grosse v Purvis*, and took, in her Honour's words, the next 'incremental step in the development of the recognition of the right to protection against, provide remedy for, breach of privacy'. [94]

Her Honour subsequently found that the defendant had breached the plaintiff's privacy by unjustifiably publishing personal information about the plaintiff and was therefore liable for damages.

The precedential value of the decisions in *Grosse v Purvis* and *Jane Doe v ABC* is still largely unknown given not only the relative recency of these decisions but also the fact that they were handed down in Courts that are limited in their ability to bind other courts. To this end, whether a tort of privacy develops beyond its infancy is contingent on its acceptance by superior courts.

To date, however, the prognosis is not encouraging. In *Giller v Procopets,* the defendant videotaped himself having sexual relations with his then partner, without her knowledge. The defendant subsequently distributed copies of the video to his friends. The plaintiff brought causes of action including, *inter alia,* an invasion of privacy. Gillard J of the Supreme Court of Victoria rejected the privacy claim finding that, whilst a cause of action in privacy is in a 'process of development'[95], it has not 'developed to a point where the law in Australia recognises an action for breach of privacy'.[96]

Similarly, in *Milne v Haynes,* Latham J of the Supreme Court of New South Wales held that 'there is, as yet, no recognition in the courts of this state of a tort of breach of privacy'.[97]

In *Kalaba v Commonwealth of Australia,* the Federal Court upheld a decision by the primary Judge in refusing to recognise that the applicant's privacy was interfered with but added that there was the 'possibility of an argument that Australian law should recognise a duty of privacy, provided that there were circumstances in which such an argument could reasonably be raised'.[98]

The experience thus far is that while Courts across the nation are open to the possibility that an actionable right to privacy *should* exist, or even *might* exist in the right circumstances, many

---

[93] *Grosse v Purvis* [2003] QDC 151, [483]

[94] *Jane Doe v Australian Broadcasting Corporation* [2007] VCC 281, [162]

[95] *Giller v Procopets* [2004] VSC 113, [187]

[96] *Giller v Procopets* [2004] VSC 113, [188]

[97] *Milne v Hayes* [2005] NSWSC 1107, [19]

[98] *Kalaba v Commonwealth of Australia* [2004] FCA 763, [8]

courts do not feel that Australian jurisprudence has evolved to the point where it can be stated definitively that a right *does* exist. The experience in *Grosse v Purvis* and *Jane Doe v ABC* are therefore the exceptions rather than the rule.

Assuming that a tort of privacy does exist, then the next question that requires elucidation is, what are the elements of this tort? Senior Judge Skoien went some way in *Grosse v Purvis* to provide a test that was adopted by Judge Hampel in *Jane Doe v ABC.* However, Senior Judge Skoien did not define the limits of a tort of privacy, nor did he exhaustively enumerate a list of defences to the tort. Judge Hampel's contribution to developing the tort of privacy was also limited, preferring to take an incremental approach. Judge Hampel refrained from deliberating on what a tort of privacy necessarily entails, having recognised its inherently imprecise nature and the difficulties in establishing an exhaustive definition.[99] In this regard, the tort of privacy in Australia remains a nascent concept, both in terms of its development (a fact acknowledged by the very Courts that gave the tort its legs) and in terms of its adoption (having only been recognised in certain situations and by relatively junior Courts).

From this experience, it appears that some time may pass before an authoritative judicial view, with far-reaching precedential value, will be established on whether a tort of privacy definitely exists in Australia.[100]

8.1 The New Zealand Experience

As a tort of privacy has not fully matured in Australia, it may be of value to refer to other jurisdictions to ascertain an understanding of the development elsewhere.

In New Zealand, the signature case is that of *Hosking v Runting.* The facts of the case are that the respondent took photographs of the appellant's infant children on a public footpath, without the plaintiff's consent. The majority of the Court of Appeal found a privacy tort exists at common law. The elements of the tort were twofold:

a) The existence of facts in which there is a reasonable expectation of privacy; and

b) Publicity given to those private facts that would be considered highly (or significantly) offensive to an objective reasonable person.

Tipping J asserted that it was:

> legally preferable and better for society's understanding of what the Courts are doing to achieve the appropriate substantive outcome under a self contained and stand-alone common law cause of action to be known as invasion of privacy.[101]

The Court held that there was no reasonable expectation of privacy as the photographs were

[99] *Jane Doe v Australian Broadcasting Corporation* [2007] VCC 281, [162]

[100] Research Note: *'Do Australians have a right to privacy?'* Department of Parliamentary Service, Parliament of Australia, 14 March 2005 at http://www.aph.gov.au/LIBRARY/pubs/rn/2004-05/05rn37.pdf, accessed 1 May 2008.

[101] *Hosking v Runting* [2005] 1 NZLR 1, [246]

taken from a public venue and that a person of ordinary sensibilities would not find the conduct highly offensive or objectionable. The Court then proceeded to dismiss the plaintiffs' appeal, as they had not demonstrated that they had met the elements of the tort.

Despite the substantial legal precedent that the Court established, the Court found that the plaintiff had failed to meet the burden of passing the test and accordingly, dismissed the appeal.

The case is important as, unlike the Australian experience, the Court did not equivocate about a supposed right to privacy but provided a definitive endorsement of its importance and existence. Further, the Court of Appeal was at the time the most senior court in New Zealand.[102] By contrast, the most senior Courts in Australia are yet to comment about the existence of a tort of privacy.

9 A STATUTORY TORT OF PRIVACY?

In May 2007, the New South Wales Law Reform Commission (NSWLRC) released a consultation paper in which the terms of reference required the Commission to consider the desirability of privacy protection principles being uniform and a consistent legislative response to privacy law, together with the desirability of introducing a statutory tort of privacy in New South Wales.

In the consultation paper, 20 questions were raised together with two proposals, including proposal 1:

> If a cause of action for invasion of privacy is enacted in New South Wales, the statute should identify its objects and purposes and contain a non-exhaustive list of the types of invasion that fall within it;[103] and

proposal 2:

> The statute should provide that where the court finds that there has been an invasion of the plaintiff's privacy, the Court may, in its discretion, grant any one or more of the following:
>
> - damages, including aggravated damages, but not exemplary damages;
> - an account of profits;
> - an injunction;
> - an order requiring the defendant to apologise to the plaintiff;
> - a correction order;
> - an order for the delivery up and destruction of material;

[102] Judgment was delivered on 25 March 2004. On 1 July 2004, the Supreme Court of New Zealand came into operation and surpassed the Court of Appeal as the most senior court in New Zealand. Many Judges from the Court of Appeal was then appointed to the Supreme Court.

[103] New South Wales Law Reform Commission, *Invasion of Privacy,* May 2007 at p 160.

- a declaration;
- other remedies or orders that the Court thinks appropriate in the circumstances.[104]

If either of the above proposals is adopted, or if some other form of statutory cause of action or invasion of privacy is enacted, this would this would offer an authoritative view currently lacking at the common law and potentially fill the gaps that exist. Any new statutory tort would possibly be more flexible and fluid in its application than the piecemeal protection currently afforded under the various legislative arrangements.[105] Work on the NSWLRC's project is continuing.

10 FUTURE DIRECTIONS

In 2004, the Office of the NSW Privacy Commissioner ('Privacy NSW') conducted a review of the *Privacy and Personal Information Protection Act 1998* (NSW) to ascertain its strengths and weaknesses, together with gauging appropriate reforms. In its report, Privacy NSW recommended comprehensive amendments to the Act and other changes relating to the functions of the Office.

It is not the intention of the paper to summarise the report in detail, but a few key issues that were raised are worth mentioning.

The report makes numerous recommendations to amend the principles to ensure and clarify that the intentions of the principles are met and the report also comments on the 'missing principles' of anonymity and limiting Government agencies from using unique identifiers. These two principles are found in the NPPs, but not the IPPs, of the *Privacy Act 1988* (Cth).

The report identified the numerous exemptions and exceptions allowed for in the *Privacy and Personal Information Protection Act 1998* (NSW) which had prompted Privacy NSW to create a 'matrix' document of these exemptions on its website.[106] The exemptions, together with the complex structure of the Act, made it difficult to understand the Act's application.[107] As a result, recommendations were made with respect to a restructure of the exemptions provided in the Act to either clarify the scope of particular exemptions or delete exemptions in the absence of clear policy reasons.[108] This would go some way to ironing out some of the problems identified regarding the 'patchwork' nature of privacy law application.

The report also recommended that the powers of the Commissioner be boosted so the Commissioner can accept whistleblower and representative complaints, as well as enabling the

---

[104] New South Wales Law Reform Commission, *Invasion of Privacy,* May 2007 at p 202.

[105] New South Wales Law Reform Commission, *Invasion of Privacy,* May 2007 at p 5.

[106] http://www.lawlink.nsw.gov.au/pc.nsf/files/privacyessentials_04.pdf/$FILE/privacyessentials_04.pdf

[107] Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998,* 24 June 2004 at p 42.

[108] Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998,* 24 June 2004 at pp 75 – 92.

Commissioner to handle freedom of information responsibilities.[109] The latter suggestion would, in effect, create an Information Commissioner with expanded functions.

11 GAPS AND OVERLAPS

The current layout of privacy law in Australia has been invariably described as 'piecemeal' and 'patchy'[110], as well as 'inconsistent' and 'fragmented'.[111] Many of the problems with privacy regulation have been assessed by numerous reviews by the relevant law reform commissions, including a current review by the Australian Law Reform Commission.

Given the absence of a definitive statement in the Australian Constitution about whether the Commonwealth Government or State Governments are responsible for privacy law, both jurisdictions are able to enact legislation with respect to personal information management.

Section 3 of the *Privacy Act 1988* (Cth) explicitly states that it does not intend to cover the field in relation to the protection of personal information. In effecting this intention, s6C of the *Privacy Act 1988* (Cth) specifically exempts State and Territory authorities from the operation of the Act. In covering the field with respect to State instrumentalities, the States of New South Wales and Victoria, together with the Northern Territory, have developed legislative schemes overseen by full time Commissioners to regulate personal information management in the relevant public sector. Other States, such as South Australia and Queensland, have adopted administrative schemes for the regulation of personal information in their respective public sectors to cover the field. [112] The result of the *Privacy Act 1988* (Cth) ceding certain responsibilities to the States and Territories has meant that a piecemeal approach to privacy protection has eventuated with the multiplicity of legislation subsequently enacted leading to both gaps and overlaps in privacy law coverage.

Firstly, there is overlap. Overlap can arise when two separate Acts that cover the same sector duplicate provisions, therefore making the provisions of one of the Acts redundant. For example, the *Health Records and Information Privacy Act 2002* (NSW) substantially overlaps with the *Privacy Act 1988* (Cth) in relation to management of health information in the private sector. A private GP in New South Wales must simultaneously adhere to the Federal NPPs and State HPPs despite a significant degree of common coverage between the two sets of principles. There is also overlap between Freedom of Information and Privacy. Section 16 of the *Freedom of Information Act 1989* (NSW) provides for a general right of access to personal files while section 14 of the *Privacy and Personal Information Protection Act 1998* (NSW) provides for a similar right of access.

Overlap also creates tension between legislation in circumstances where there is a requirement

---

[109] Privacy NSW, *Submission on the Review of the Privacy and Personal Information Protection Act 1998,* 24 June 2004 at pp 75 – 92.

[110] Carolyn Doyle & Mirko Bagaric, *Privacy Law in Australia,* The Federation Press 2005 at p 178.

[111] The Australian Law Reform Commission's *Issues Paper 31; Review of Privacy – Discussion Paper 72* dedicated a whole chapter on the 'Interaction, Fragmentation and Inconsistency of Privacy Regulation'.

[112] Australian Law Reform Commission, *Review of Australian Privacy Law – Discussion Paper 72,* September 2007 at p 520.

under one Act without that requirement being mirrored in the sister legislation. In one of the examples raised above, the *Health Records and Information Privacy Act 2002* (NSW) specifies the form of access that organisations must provide when individuals seek their health information, whereas the *Privacy Act 1998* (Cth) does not stipulate how access is to be effected. In this respect, a GP may be compliant with one Act but be found to be in breach of the other.

Multiple pieces of legislation also lead to fragmentation. For example, the Information Protection Principles apply to the public sector in NSW whilst the Information Privacy Principles apply to the public sector federally. Although both principles ostensibly apply to their relevant public sectors, each set of principles is different. Meanwhile, the *Privacy Act 1988* (Cth) also includes the National Privacy Principles to cover parts of the private sector. The result is that in New South Wales there are three sets of privacy principles covering three different sectors. While divergence in the wording between the different sets of principles may simply be a distinction without difference, the lack of a consistent definition leads to an overall sense of fragmentation.

In its *Review of Privacy*, the Australian Law Reform Commission found that there was strong support for the development of consolidated principles that are nationally consistent.[113] In its submission to the review, Privacy NSW also agreed that uniform privacy laws developed in a cooperative Federal – State framework were highly desirable in creating an integrated national privacy regime.[114] The nationally consistent laws – referred to as Unified Privacy Principles in the *Review of Privacy*[115] – would presumably combine to cover both public sectors, together with the private sector. The UPPs may also be modelled on the current NPPs as they are more comprehensive than the IPPs and are framed in language that is more relevant and contemporary.

Despite the combined application of the *Privacy Act 1988* (Cth) and the *Privacy and Personal Information Protection Act 1998* (NSW), there are still regulatory black holes in certain situations. For example, the *Privacy and Personal Information Protection Act 1998* (NSW) does not cover state owned corporations. As state owned corporations also fall outside the remit of the *Privacy Act 1988* (Cth) unless prescribed by regulation, the result is that state owned corporations fall in between the unregulated gap between the *Privacy Act 1988* (Cth) and the *Privacy and Personal Information Protection Act 1998* (NSW), effectively rendering these entities free from compliance with any privacy standard.

There is also confusion as to whether contracted service providers to State Government agencies are covered by the *Privacy and Personal Information Protection Act 1998* (NSW).[116] Under the *Privacy Act 1988* (Cth), contracted service providers to State Government agencies are exempt from the NPPs.[117] However, under section 12(d) of the *Privacy and Personal Information*

---

[113] Australian Law Reform Commission, *Review of Australian Privacy Law – Discussion Paper 72,* September 2007 at pp 238 – 241.

[114] Privacy NSW, *Review of Privacy Discussion Paper 72 of the Australian Law Reform Commission,* December 2007 at p 6.

[115] Australian Law Reform Commission, *Review of Australian Privacy Law – Discussion Paper 72,* September 2007 at p 544.

[116] Australian Law Reform Commission, *Review of Privacy Issues Paper 31,* October 2006 at p 343.

[117] *Privacy Act 1988* (Cth) s 6F

Protection Act 1998 (NSW), a public sector agency that holds personal information must only ensure that, 'if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or disclosure of the information'. [118] There is ambiguity as to the scope and meaning of this provision and it is possible that contracted service providers to NSW Government agencies also fall within the unregulated gap between the State and Federal Acts.

Businesses that have an annual turnover of less than $3 million are also exempted from the NPPs in the *Privacy Act 1988* (Cth) and are not covered by the *Privacy and Personal Information Protection Act 1998* (NSW). Similarly, private organisations are exempt from *Privacy Act1988* (Cth) compliance insofar as it relates to an employee's employment relationship. While the State Government is able to legislate to cover the field with respect to small businesses and employee records, during the discussion about the development of the *Privacy and Personal Information Protection Act 1998* (NSW), it was decided that a nationally consistent approach was preferable and best left at the discretion of the Federal Government.[119]

12 NEW AND EMERGING TECHNOLOGIES

Changes in the privacy landscape have almost always been influenced by technological development. The famous Warren and Brandeis article was prompted by concerns about the use of the emerging technology of the time, the instantaneous photograph.[120] Later, in the ALRC landmark review of privacy in 1983, there was discussion about the emerging possibilities (and threats) brought about by what it described as 'information processing' and the 'marriage of the computer revolution with telecommunications, the era of *computications*'.[121]

Today, concerns about further technological development in the fields of IT, biometrics and tracking devices influence discussions about privacy. In this context, privacy is emerging at the leading edge of academic discussion as more people are ascribing added degrees of importance to protecting their privacy. In the fictional TV series *The West Wing*, the Deputy Communications Director, Sam Seaborn, tells the President during a discussion about the emerging importance of privacy:

> It's about the next 20 years. Twenties and thirties, it was the role of government. Fifties and sixties, it was civil rights. The next two decades, it's gonna be privacy. I'm talking about the Internet. I'm talking about cellphones. I'm talking about health records, and who's gay and who's not. And moreover, in a country born on a will to be free, what could be more fundamental than this?

New technologies are not necessarily destructive of privacy, but misuse of the new technologies can have privacy-intrusive consequences that can 'distort the balancing act between individual

---

[118] *Privacy and Personal Information Protection Act 1998* (NSW) s 12(d)

[119] The Hon. J. W. Shaw in NSWPD, 17 September 1998 at p 7601.

[120] LD Brandeis and SD Warren, 'The right to privacy' (1890) *4 Harvard Law Review* 193 at p 193.

[121] The Law Reform Commission, *Privacy,* Report No 22, 1983 at pp 43 – 44.

privacy and other social needs'.[122] Listed below are some examples of current and emerging technologies whose use or misuse can be privacy-intrusive and which regulators need to consider as the next possible frontier in protecting personal privacy.

12.1 Biometrics

Biometrics is the umbrella term that describes the biological measurements used to identify or authenticate humans.[123] Biometric applications essentially work by taking a sample from an individual, converting it into a template and storing it on a database.[124] Subsequent biometric samples from the individual can then be used to identify or verify the individual by matching subsequent collections with the stored data.

Examples of biometric applications include capturing fingerprints, retinal and iris scans, analysis of hand geometry and ear lobe capillary structures, facial structure and voice recognition. Biometrics can also capture both the behavioural and psychological aspects of individuals, such as keystroke dynamics, hand writing technique and movement technique.

Biometric applications are not privacy intrusive per se, but have the potential to have a negative impact on personal privacy, even if the user is not deliberately attempting to use to the application in a privacy-invasive manner.

One concern about biometric technology is that it has the potential to lead to widespread surveillance of people given the relative ease in capturing and storing the data, and being able to 'match' the stored data with the relevant subject.[125] As biometric information is highly reliable and unique, disparate biometric data can easily be consolidated to create comprehensive profiles of any one individual.

A second concern is that biometrics can be used to identify people without their knowledge or consent.[126] The concern emerges from the fact that biometric information is capable of being collected covertly, such as capturing a digitised image of someone's face or through keystroke monitoring.

Also, when biometric information is collected, it may result in the collection of more information than was intended. For example, if a person submits to an iris scan for the purposes of authenticating the individual, the scan may also unintentionally reveal eye conditions the person has if analysed by an iridologist. Similarly, a voice recording may reveal a person's emotional state.[127] Essentially, the human body contains hidden messages embedded in our biometric data

---

[122] Malcolm Crompton, *Under the Gaze, Privacy Identity and New Technology,* Speech at the Union Internationale des Advocats (International Union of Lawyers), 75th Anniversary Congress, 2002 Sydney at p 9.

[123] Roger Clarke, *Biometrics and Privacy* at http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html, accessed 8 July 2008.

[124] Australian Law Reform Commission, *Review of Privacy Issues Paper 31,* October 2006 at p 523.

[125] Ibid at p 525.

[126] Ibid.

[127] Malcolm Crompton, *Under the Gaze, Privacy Identity and New Technology,* Speech at the Union

which can be revealed through a more detailed analysis of an otherwise innocuous sample.

In Australia, biometric technology is being introduced gradually. The Australian Government has introduced the 'ePassport' system that includes, among other things, a digitised facial image of the passport holder. The passport holder is now able to proceed through a 'smartgate' that uses facial recognition software to verify that the person passing through the gate matches the digitised facial image on the passport. Businesses frequently use biometric applications for security purposes, such as accessing secure rooms or logging on to computer programs. As biometrics become more commonplace, the possible threats to privacy also increase.

12.2 Location-Based Technologies

Radio frequency identification (RFID) works by chipping a tag in a product, animal or person for the purposes of identification and tracking by emitting radio waves that can be read by a radio scanner.

RFID technology is not new and its use in tagging clothes in department stores to prevent theft is long established. If the tagged clothing item is stolen, the RFID reader at the exits detects the radio waves being emitted by the RFID tag on the clothing and the match then triggers an alarm. Similarly, tollways use RFID technology to detect passing vehicles fitted with a RFID tag ('e-tag') and deduct the fee from the toll users' account.

As these two examples demonstrate, RFID technology has many uses and its application has been important in minimising loss and theft and maximising speed and efficiency. However, RFID technology can also be used to surreptitiously collect a variety of data. RFID tags are able to transmit data that identifies not only the object to which it is attached, but also such things such as its location, price, expiry data, colour, or date of purchase of product.[128] RFID tags may also be able to transmit data about its surroundings.[129]

The primary concern about RFID technology is that it may be used covertly to identify individuals that buy certain products, for example books or suits. There have also been reports that RFID technology is being employed to locate the whereabouts of individuals, similar to the way one can microchip a pet. Recently, a school in England advised it may begin using RFID tags attached on to the uniforms of some of its students to monitor their whereabouts in an attempt to rein in truancy rates.[130]

Also, the advent and popularity of the global positioning system (GPS) has enabled millions of people to accurately locate themselves through the use of satellite technology by GPS systems either in their cars or phones. Although ostensibly used for navigational purposes, GPS and its location detecting abilities can also be used to surreptitiously collect information about the

---

Internationale des Advocats (International Union of Lawyers), 75th Anniversary Congress, 2002 Sydney at p 17.

[128] Australian Law Reform Commission, *Review of Privacy Issues Paper 31,* October 2006 at p 529.

[129] Ibid.

[130] Nicola Woolcock. *Microchip gives staff the lowdown on pupils,* Times Online, 20 October 2007 at http://www.timesonline.co.uk/tol/news/uk/education/article2698062.ece

whereabouts of individuals.

12.3 The Internet

The Internet represents one of the most potent threats against privacy today. The innate nature of IT means that personal data can be accessed, replicated and disclosed anywhere in the world, in a matter of seconds.

The huge popularity of personal websites and integrated networking sites, such as Facebook, has given privacy on the Internet a new meaning. Websites like these enable individuals to upload information and photographs about themselves and others. This could be quite privacy intrusive, especially if the information or photograph is embarrassing or offensive.

Other privacy issues that relate to the internet include the use of spyware, a software that enables a third party to effectively view information stored or activity undertaken on a computer. The monitoring is often without the consent of the user and the surreptitious collection of information can be used to commit identity theft, fraud or send spam. Spyware effectively monitors web-surfing activities and, in doing so, has obvious privacy implications.

Cookies also present a hazard to privacy as they are small files on the computer that can be accessed by websites visited by the user. Some website operators use cookies to gather information about a user and share this information with partner websites. On occasion, a cookie could be installed on a computer, without the user's knowledge or permission, and used to collect information about that person's web surfing habits for advertising or marketing purposes.

Phishing emails are often sent to acquire personal details such as bank account details and 'Trojan Horses' can similarly be uploaded onto computers and used to monitor keystrokes to steals the passwords and PINS of accounts.

Changes in IT have had an effect on how individuals perceive cyberprivacy. In a recent OPC survey, 50% of Australians were more concerned about providing information over the Internet than they were in 2004.[131] At that time, 62% described themselves as having more concerns about the security of their personal information online than before. [132]

13 CONCLUSION

When Zelman Cowen delivered the 1969 Boyer lectures, titled 'The Private Man', he famously declared: 'A man without privacy is a man without dignity'. [133] The concern about privacy of the individual has not diminished in the 39 years since Cowen spoke those words. If anything, it has been exacerbated. Threats in contemporary society together with ongoing technological development have meant that privacy has evolved as a concern in the minds of many and faces an important period of change and challenge ahead.

---

[131] Ibid.

[132] Ibid.

[133] Zelman Cowen, 1969 Boyer Lecture in Independent Commission Against Corruption, *Report on unauthorised release of Government information: Volume I,* August 1992 at p 20.

Recent Research Service Publications

To anticipate and fulfil the information needs of Members of Parliament and the Parliamentary Institution.

[Library Mission Statement]

Note: **For a complete listing of all Research Service Publications contact the Research Service on 9230 2093. The complete list is also on the Internet at:**

http://www.parliament.nsw.gov.au/prod/web/PHWebContent.nsf/PHPages/LibraryPublist

BACKGROUND PAPERS

The Science of Climate Change by Stewart Smith 1/06
NSW State Electoral Districts Ranked by 2001 Census Characteristics by Talina Drabsch 2/06
NSW Electorate Profiles: 2004 Redistribution by Talina Drabsch 3/06
Parliamentary Privilege: Major Developments and Current Issues by Gareth Griffith 1/07
2007 NSW Election: Preliminary Analysis by Antony Green 2/07
Manufacturing and Services in NSW by John Wilkinson 3/07
2007 New South Wales Election: Final Analysis by Antony Green 1/08

BRIEFING PAPERS

Tobacco Control in NSW by Talina Drabsch 1/05
Energy Futures for NSW by Stewart Smith 2/05
Small Business in NSW by John Wilkinson 3/05
Trial by Jury: Recent Developments by Rowena Johns 4/05
Land Tax: an Update by Stewart Smith 5/05
No Fault Compensation by Talina Drabsch 6/05
Waste Management and Extended Producer Responsibility by Stewart Smith 7/05
Rural Assistance Schemes and Programs by John Wilkinson 8/05
Abortion and the law in New South Wales by Talina Drabsch 9/05
Desalination, Waste Water, and the Sydney Metropolitan Water Plan by Stewart Smith 10/05
Industrial Relations Reforms: the proposed national system by Lenny Roth 11/05
Parliament and Accountability: the role of parliamentary oversight committees by Gareth Griffith 12/05
Election Finance Law: an update by Talina Drabsch 13/05
Affordable Housing in NSW: past to present by John Wilkinson 14/05
Majority Jury Verdicts in Criminal Trials by Talina Drabsch 15/05
Sedition, Incitement and Vilification: issues in the current debate by Gareth Griffith 1/06
The New Federal Workplace Relations System by Lenny Roth 2/06
The Political Representation of Ethnic and Racial Minorities by Karina Anthony 3/06
Preparing for the Impact of Dementia by Talina Drabsch 4/06
A NSW Charter of Rights? The Continuing Debate by Gareth Griffith 5/06
Native Vegetation: an update by Stewart Smith 6/06
Parental Responsibility Laws by Lenny Roth 7/06
Tourism in NSW: Prospects for the Current Decade by John Wilkinson 8/06
Legal Recognition of Same Sex Relationships by Karina Anthony and Talina Drabsch 9/06
Uranium and Nuclear Power by Stewart Smith 10/06
DNA Evidence, Wrongful Convictions and Wrongful Acquittals by Gareth Griffith and Lenny Roth 11/06
Law and Order Legislation in the Australian States and Territories: 2003-2006 by Lenny Roth 12/06
Biofuels by Stewart Smith 13/06
Sovereign States and National Power: Transition in Federal- State Finance by John Wilkinson 14/06
Reducing the Risk of Recidivism by Talina Drabsch 15/06
Recent Developments in Planning Legislation by Stewart Smith 16/06
Commonwealth-State Responsibilities for Health – 'Big Bang' or Incremental Reform? by Gareth Griffith 17/06

The* Workplace Relations Case – *Implications for the States
by Lenny Roth and Gareth Griffith 18/06
Crystal Methamphetamine Use in NSW by Talina Drabsch 19/06
Government Policy and Services to Support and Include People with Disabilities
by Lenny Roth
1/07
Greenhouse Gas Emission Trading by Stewart Smith 2/07
Provocation and Self-defence in Intimate Partner and Homophobic Homicides
by Lenny Roth 3/07
Living on the Edge: Sustainable Land Development in Sydney by Jackie Ohlin 4/07
Women, Parliament and the Media by Talina Drabsch 5/07
Freedom of Information: Issues and Recent Developments in NSW by Gareth Griffith 6/07
Domestic Violence in NSW by Talina Drabsch 7/07
Election Finance Law: Recent Developments and Proposals for Reform
by Gareth Griffith and Talina Drabsch 8/07
Multiculturalism by Lenny Roth 9/07
Protecting Children From Online Sexual Predators by Gareth Griffith and Lenny Roth 10/07
Older Drivers: A Review of Licensing Requirements and Research Findings
by Gareth Griffith 11/07
Liquor Licensing Laws: An Update by Lenny Roth 12/07
Residential Tenancy Law in NSW by Gareth Griffith and Lenny Roth 13/07
The NSW Economy: A Survey by John Wilkinson 14/07
The NSW Planning System: Proposed Reforms by Stewart Smith 1/08
Carbon Capture and Storage by Stephanie Baldwin 2/08
A Commissioner for Older People in NSW? by Gareth Griffith 3/08
Education in Country and City NSW by John Wilkinson 4/08
The Regulation of Lobbying by Gareth Griffith 5/08
Transport Problems Facing Large Cities by Tom Edwards and Stewart Smith 6/08
Privacy: the Current Situation by Jason Arditi 7/08