Electronic workplace surveillance and employee privacy – A comparative analysis of privacy protection in Australia and the United States.

James Robert Watt, B.Inf (Griff), B.Econ (Qld), LL.B (QUT).
Barrister-at-Law

Submitted in fulfilment of the requirements for the degree of Master of Laws in the Faculty of Law, Queensland University of Technology 2009.

CONTENTS

KEYWORDS

Workplace privacy, employee privacy rights, electronic monitoring, workplace surveillance, video surveillance, Internet and email monitoring, Privacy Act, information privacy, Fourth Amendment, Intrusion Upon Seclusion, technology and privacy, privacy tort, reasonable expectation of privacy, invasion of privacy, workplace privacy legislation.

ABSTRACT

More than a century ago in their definitive work "The Right to Privacy" Samuel D. Warren and Louis D. Brandeis highlighted the challenges posed to individual privacy by advancing technology. Today's workplace is characterised by its reliance on computer technology, particularly the use of email and the Internet to perform critical business functions. Increasingly these and other workplace activities are the focus of monitoring by employers.

There is little formal regulation of electronic monitoring in Australian or United States workplaces. Without reasonable limits or controls, this has the potential to adversely affect employees' privacy rights.

Australia has a history of legislating to protect privacy rights, whereas the United States has relied on a combination of constitutional guarantees, federal and state statutes, and the common law. This thesis examines a number of existing and proposed statutory and other workplace privacy laws in Australia and the United States.

The analysis demonstrates that existing measures fail to adequately regulate monitoring

or provide employees with suitable remedies where unjustifiable intrusions occur. The thesis ultimately supports the view that enacting uniform legislation at the national level provides a more effective and comprehensive solution for both employers and employees.

Chapter One provides a general introduction and briefly discusses issues relevant to electronic monitoring in the workplace. Chapter Two contains an overview of privacy law as it relates to electronic monitoring in Australian and United States workplaces. In Chapter Three there is an examination of the complaint process and remedies available to a hypothetical employee (Mary) who is concerned about protecting her privacy rights at work. Chapter Four provides an analysis of the major themes emerging from the research, and also discusses the draft national uniform legislation. Chapter Five details the proposed legislation in the form of the Workplace Surveillance and Monitoring Act, and Chapter Six contains the conclusion.

TABLE OF CONTENTS

STATEMENT OF ORIGINAL AUTHORSHIP

I have not previously submitted the work contained in this thesis to meet requirements for an award at this or any other higher education institution. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made.

_____
James Robert Watt

_____
Date

Chapter One

Introduction

"Everything we do today creates a transaction where it didn't before." [1]

Through seemingly innocuous everyday transactions, we create an electronic trail that allows others to monitor and record our lives. Such scrutiny is increasingly prevalent in the workplace.

Gross states that a legal interest in privacy exits where a person is concerned about their privacy and there is legal recognition of such concern. [2] However, "[t]he law does not determine what privacy is, but only what situations of privacy will be afforded legal protection, or will be made private by virtue of legal protection." [3] Though, "…privacy in these contexts does not exist because of such legal recognition. It exists – like secrecy, security, or tranquillity – by virtue of habits of life appropriate to its existence." [4]

Information privacy is concerned with preserving the confidentiality of information, and is therefore the most relevant kind of privacy with respect to Internet and email monitoring. [5] Arguably, this reasoning extends to all forms of electronic monitoring.

Electronic monitoring raises some important challenges to the conventional information privacy model. Modern technology permits the seamless collection and storage of vast amounts of diverse personal information, often without the consent or knowledge of the individual concerned, or without the need to demonstrate that the collection is for a legitimate business purpose.

---

1 Bruce Schneier, Chief Technology Officer, BT Counterpane in Carly Weeks, 'No escaping Big Brother's watchful eyes and ears: Privacy experts warn of a future in which everything we do can be recorded and stored', *The Edmonton Journal* (Edmonton), September 28, 2007.
2 Hyman Gross, 'The Concept of Privacy' (1967) 42 *New York University Law Review* 34, 36.
3 Ibid.
4 Ibid.
5 Hazel Oliver, 'Email and Internet Monitoring in the Workplace: Information Privacy and Contracting-Out' (2002) 31(4) *Industrial Law Journal* 321, 322.

Performance appraisal, security, and protection from litigation are just some of the many uses made of information collected through monitoring. Unfortunately, much of the information acquired in this manner falls outside the scope (and protection) of current information privacy laws.

In 2005 a survey of 526 American corporations found 76% monitored employees' Internet connections, 50% stored and reviewed employees' computer files, and 55% reported retaining and reviewing email messages. [6] The extent of monitoring in Australia is more difficult to discern, however, in 2000 the Australian National law firm Freehill, Hollingdale and Page reported that 76% of respondent employers periodically monitored the content of employees' emails, while 5% monitored emails on a regular basis. [7] A study in 2004 by the NSW State Chamber of Commerce and the Unisys Corporation found that of those employers who had policies on the use of computing facilities only 16% used technological means to monitor compliance. [8]

In Australia, electronic monitoring remains largely unregulated. Only New South Wales and Victoria have enacted workplace privacy laws. [9] Meanwhile changes in technology are lowering the cost and increasing the effectiveness of conducting monitoring. This raises concerns over the impact this increasing reliance on monitoring may have on employees' privacy rights.

Objectives

The thesis has three main objectives: to discuss the impact of electronic monitoring on employees' privacy rights; to analyse and compare the current complaint processes and

---

6 American Management Association, *2005 Electronic Monitoring & Surveillance Survey* <http://www.amanet.org/research/pdfs/EMS_summary05.pdf> at 8 March 2006.

7 Freehill Hollingdale & Page, 'Internet Privacy Survey Report 2000' in Lenny Roth, 'Workplace Surveillance - Briefing Paper No. 13/04' New South Wales Parliamentary Library Research Service (2004), 23-4. See also 'Internet privacy survey shows Australian websites lacking – Freehills Internet Privacy Survey Report 2000' [2000] PLPR 1.

8 Ibid 24 (Referencing State Chamber of Commerce (NSW) and Unisys, 'Getting a Grip on the Internet: Information Technology Survey'). The Australian surveys were less extensive with 67 of Australia's top 200 companies responding to the Freehills' survey, whilst the Chamber of Commerce findings were based on a survey of approximately 100 businesses.

9 *Workplace Surveillance Act 2005* (NSW); *Surveillance Devices (Workplace Privacy) Act 2006* (Vic).

remedies available to Australian and United States employees for intrusions caused by electronic monitoring; and to propose a uniform legislative strategy to regulate electronic monitoring in Australian workplaces. [10]

Much of the discussion on this topic focuses on developing a theoretical framework to evaluate the often complex issues raised. Whilst acknowledging the value of such analysis, this thesis instead adopts a more functional approach, including providing a case study model accompanied by suggested draft legislation.

The research involves an analysis of the extent to which existing and proposed legislative measures in both Australia and the United States protect employees' privacy rights. There is also an examination of constitutional and tort privacy in the United States, and the development of a cause of action at common law for invasion of privacy in Australia.

The United States has an eclectic mix of privacy regulation that offers significant insight into the effectiveness of differing legal approaches in addressing privacy concerns in the workplace. Although there is minimal statutory protection, the courts have a long history of applying constitutional guarantees and the common law to invasions of privacy. There have also been several unsuccessful attempts to enact national workplace privacy legislation.

In Australia, the Commonwealth and most states have enacted information privacy legislation. However, there is no specific workplace privacy legislation at the federal level, and it is only relatively recently that the courts have revisited a cause of action at

[10] For a definition of electronic monitoring, see the draft Bill (Chapter Five). In this thesis I do not distinguish between the terms "electronic monitoring" and "surveillance" for with both "…there is the connotation of intentionally watching, listening to, recording or otherwise collecting information about people…" (Victorian Law Reform Commission, *Workplace Privacy Options Paper* (2004), [2.2]). See also Neville Meyers, 'If Big Brother comes to a venue near you! Employee-surveillance issues and the communication professional' (2003) 30(2) *Australian Journal of Communication* 101, 103 (Citing the International Labour Office). Note though that the terms can have different meanings: see Carl Botan and Mihaela Vorvoreanu, 'What do Employees Think about Electronic Surveillance at Work?' in John Weckert, (ed.), *Electronic Monitoring in the Workplace: Controversies and Solutions* (2005), 125 (and references therein).

common law.

Existing information privacy legislation is insufficient to address the issues raised by electronic monitoring. In addition, neither the New South Wales nor the Victorian measures provide comprehensive protection to employees. In the United States constitutional, legislative and common law privacy protections have also failed to offer employees sufficient redress. A national uniform legislative strategy will provide a comprehensive framework to regulate electronic monitoring and ensure the effective protection of employees' privacy rights.

The Concept of Workplace Privacy

Providing a conclusive definition of privacy in general has proven elusive. Privacy has "…psychological, social and political dimensions which reach far beyond its analysis in the legal context;…." [11] The concept of privacy is variously defined to encompass amongst other things mental repose, physical solitude, physical exclusiveness, autonomy, [12] as a fundamental human right, [13] a property right, [14] and as an economic right. [15]

Privacy is also concerned with an individual's right to control his or her own information. [16] Thus, employees should expect to have some level of control over personal information collected by their employer through monitoring.

---

[11] Edward J. Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 *New York University Law Review* 962, 963 (and references therein).

[12] Gross, above n 2, 37-9.

[13] See Global Internet Liberty Campaign, 'Privacy and Human Rights: An International Survey of Privacy Laws and Practice' <http://www.gilc.org/privacy/survey/exec-summary.html> at 28 March 2008. The survey examined constitutional and legal conditions of privacy protection in fifty countries and noted the widespread recognition of privacy as a fundamental human right in state constitutions and international treaties.

[14] See Lawrence E. Rothstein, 'Privacy or Dignity?: Electronic Monitoring in the Workplace' (2000) 19 *New York Law Journal of International and Comparative Law* 379, 381-2 (citing Ernest Van Den Haag).

[15] Richard A. Posner, 'The Right of Privacy' (1977-8) 12(3) *Georgia Law Review* 393.

[16] See Meyers, above n 10, 103, (citing Westin); Lilian Mitrou and Maria Karyda 'Employees' privacy vs. employers' security: Can they be balanced?' (2006) 23 *Telematics and Informatics* 164, 167 (cites Westin and others).

Privacy rights are contingent upon factors such as circumstance, location and activity, and a person will have a different expectation of privacy at work as opposed to other locations, such as the home. [17] Even though a person's expectation of privacy may not be as extensive in the workplace, it is reasonable for employees to expect some level of protection against unwarranted intrusions caused through their employer's use of electronic monitoring.

Addressing privacy concerns in the workplace is important for a number of reasons. "Work is one of the most fundamental aspects in a person's life, …." [18] As such "…the conditions in which a person works are highly significant in shaping the whole compendium of psychological, emotional and physical elements of a person's dignity and self respect." [19]

In addition, the hours worked by full time Australian workers have increased over the last 20 years. The Australian Bureau of Statistics reports that in 2005 there were 30% of male workers and 16% of female workers working 50 hours or more a week (compared with 22% and 9% respectively in 1985). [20] If employees have less time to conduct private activities outside work hours, this could lead to an increased use of employer supplied computer equipment for personal reasons. As a result, a greater number of activities engaged in by employees may become subject to monitoring.

It is widely acknowledged that employers have a legitimate interest in monitoring employment related activities in the workplace. This includes the need to evaluate employees' performance, to limit potential legal liability, or to protect employees through ensuring the implementation of appropriate health and safety procedures. The aim here is not to argue for the subrogation of these rights, but instead to attempt to identify and elucidate the legal issues involved.

---

17 Andrew J. Charlesworth, 'Privacy, Personal Information and Employment' (2003) 1(2) *Surveillance & Society* 217, 217-8.

18 *Reference Re Public Service Employee Relations Act* [1987] 1 S.C.R. 313, 368 (Dickson C.J, Wilson J dis).

19 Ibid.

20 Australian Bureau of Statistics, 'Australian Social Trends 2006, Trends in Hours Worked' (Cat. No. 4102.0).

This is particularly relevant given that the pace of technological change, coupled with the absence of appropriate controls, poses significant challenges to employees' privacy rights however constituted. As such, even though these rights (and those of their employers) may elude precise definition, they are nonetheless worthy of legal recognition.

Electronic Monitoring Technology

Employers use a wide variety of technologies to monitor employees in the workplace. The focus here is on electronic mail (email), the Internet, and closed circuit television cameras ("CCTV").

The Internet is a global communications network that facilitates the sending, receiving, and storing of information. [21] Communications transmitted over the Internet are comprised of two constituent elements, the actual content, and the addressing information used to deliver the communication. [22] Before transmitting the information, the system separates each communication into packets. [23] Email is one form of electronic communication sent though the Internet. The content information of an email is the message itself, whilst the addressing information is contained in the header. [24] Thus, email monitoring can reveal address information about the sender and recipient, the subject of the email, and other details including the content of the message.

Users compose email messages using a client program. [25] One element of the server's mail processing application breaks the message down into packets, and another sends the packets out through the Internet. [26] The message passes through various servers before reaching its final destination, with computers at each intermediate stage storing the

---

21 See Orin S. Kerr, 'Internet Surveillance Law after the USA Patriot Act: The Big Brother that Isn't' (2003) 97 *Northwestern University Law Review* 607, 610.

22 Ibid 611.

23 Ibid 613 (Citing Preston Gralla).

24 Ibid 612. Addressing information includes details of the sender, recipient, date, subject and the path the message has taken in order to reach its destination.

25 *United States v. Councilman*, 418 F.3d 67, 69 (1st Cir. 2005) (Lipez J). Microsoft Outlook is a popular email client program.

26 Ibid.

packets in memory, examining the addresses and delivering to the next node of the network. [27] Sometimes a computer will not immediately forward the received messages but store them for some time before sending to the next node. [28] Finally, the destination server's software receives the message, identifies the recipient, and places the message in that users' inbox. [29]

Surveillance can either be "prospective" - focusing on future communications, or "retrospective" - capturing data already retained in the system. [30] The former approach may result in the acquisition of some irrelevant data, while the later is limited to existing records. [31]

Employees usually connect to the Internet through their employer's local area network ("LAN"). The LAN comprises a server(s) and desktop computers, printers and other peripherals. Access to the LAN is usually by username and password. The employee can then access applications, send emails, and use the Internet.

An employer may choose to monitor any or possibly all of these activities. Modern monitoring software has quite extensive capabilities. This includes the ability to record keystrokes, log emails sent and received, screen emails for offensive or inappropriate content, take snapshots of the desktop at set times, and track programs run by users. [32] Surveillance of the Internet conducted "at the packet level" can capture information such as the type of communication (web page, picture, text file), as well as the Internet addresses of the sending and receiving computers. [33]

---

27 Ibid 69-70 (Citing J Klensin). This process includes disassembly and reassembly of the packets where required.

28 Ibid 70. This is known as the " 'store and forward' " method of transmission. Even when there is no delay, intermediate servers often retain copies of the message which are subsequently deleted.

29 Ibid.

30 Kerr, above n 21, 616.

31 Ibid 616-7 (and references therein).

32 See H. Joseph Wen and Pamela Gershuny, 'Computer-based monitoring in the American workplace: Surveillance technologies and legal challenges' (2005) 24 *Human Systems Management* 165, 167; G. Daryl Nord, Tipton F. McCubbins and Jeretta Horn Nord, 'E-Monitoring in the Workplace: Privacy, Legislation, and Surveillance Software' (2006) 49(8) *Communications of the ACM* 73, 75.

33 Kerr, above n 21, 614 (Quoting Vincenzo Medillo and others).

CCTV cameras can acquire images (either analogue or digital) via a cable or wireless link and transmit "…to a monitor- recording device of some sort, where they are available to be watched, reviewed and/or stored." [34] Cameras use different methods to record resulting in a variance in the quality of the captured image. [35] The storage method and manner in which images are manipulated "…have different implications as regards the type and speed of monitoring that can be carried out." [36]

Modern CCTV cameras are "…active devices that can be manipulated to trace an individual's movements within the camera zone, and…communicate with each other to ensure continuous coverage as individuals move from one camera area to another." [37] So called "intelligent" cameras now in development will possess additional functions, such as facial recognition and the ability to analyse images and detect possible threats to safety and security. [38] In addition, "…cameras are becoming smaller, less expensive and more readily available." [39]

Australian Law

Telecommunications Interception and Access Act

The *Telecommunications (Interception and Access) Act 1979* (Cth) prohibits (except in certain limited circumstances) the interception of communications "passing over a telecommunications system." [40] The interception must occur while the communication is in transit. [41] Law enforcement and security agencies can obtain a warrant to intercept communications or access communications that are stored on equipment belonging to

---

[34] Martin Gill and Angela Spriggs, 'Assessing the Impact of CCTV' (2005) Home Office Research Study 292, 1-2.
[35] Ibid 2.
[36] Ibid 2.
[37] Avner Levin, Mary Jo Nicholson, 'Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground' (2005) 2 *University of Ottawa Law and Technology Journal* 357, 368.
[38] See Rene Bruemmer, 'Why are Cameras Corrosive of Liberties?' (2007) 33(11) *Privacy Journal* 1, 5; Clifton Coles, 'Fighting Crime with Closed-Circuit Cameras' (2005) *The Futurist* 10; Stephen Manning, 'Security cameras get eyes, brains', *Sydney Morning Herald*, (Sydney), 12 April 2007.
[39] Victorian Law Reform Commission, above n 10, [2.6].
[40] ss 6(1), 7(1),(2). The Act also prohibits using or communicating intercepted information: s 63.
[41] s 5F(1), 6(1).

telecommunications carriers. [42] Unlawfully intercepting a communication is an indictable offence punishable by imprisonment for a period not exceeding 2 years. [43] Unlawfully accessing stored communications is punishable by imprisonment for 2 years, 120 penalty units, or both. [44] Civil remedies are also available. [45]

There are a number of concerns with respect to the level of protection the Act may afford employees. For example, an interception that occurs through monitoring communications may be lawful where a person is aware of the monitoring. [46] Also, depending on the interpretation of the requirement that an interception occur whilst the communication is "…passing over a telecommunications system…" an employer may be able to read an employee's email messages without breaching the Act. [47]

If an employer's network comprises a stand-alone system separate from the carrier's network, then the Act may apply to accessing employees' emails. [48] In addition, employers may be able to lawfully access communications residing on systems they own and manage as long as at the time of access the communication is not " 'passing over a telecommunications system.' " [49]

The Act focuses on protecting the privacy of individuals using telecommunications services (through creating offences for unlawful interception and access) and regulating

---

42 See ss 5(1), 6E-EB, Parts 2-2, 2-5, 3.3. For a technical analysis of interceptions and the Internet see Philip Branch, 'Lawful Interception of the Internet' (2003) 1(1) *Australian Journal of Emerging Technologies and Society* 38.

43 s 105(2).

44 s 108(1).

45 ss 107A (interception), 165 (unlawful access).

46 s 6(1). The Act requires an interception be "…without the knowledge of the person making the communication." See also Victorian Law Reform Commission, *Workplace Privacy Issues Paper* (2002), [4.13].

47 Ibid. This is due to the technology involved in sending emails. If "passing over" is defined to be the journey between the sending and receiving computer then accessing an email temporarily stored on an intermediate server (network or ISP) would be an interception. However, if "passing over" is restricted to the transit through the cables or fibre then access on the server would not constitute an interception.

48 Ibid. This relates to the definitions in section 5 of a telecommunications network as "…a system, or series of systems, for carrying communications…" and a telecommunications system as "…a telecommunications network that is within Australia;…."

49 See Andrew Schatz, 'Recent developments in telecommunications interception and access law' Australian Government Solicitor, Commercial Notes No. 20 (19 September 2006), 3. Access includes "…listening to, reading or recording… a communication" (s 6AA). Section 5F defines what constitutes "passing over a telecommunications system."

lawful interceptions and access to stored communications (through the issuance of warrants). [50] In conjunction with the above concerns, this means it offers employees limited protection against electronic monitoring and is not further discussed.

Information Privacy

The *Privacy Act* provides a comprehensive framework for implementing the information privacy guidelines adopted by the Organisation for Economic Co-operation and Development. [51] The legislation is also relevant to Australia's obligations under Article 17 of the *International Covenant on Civil and Political Rights*. [52]

The *Privacy Act* regulates the collection, use, storage, and disclosure of personal information held by government agencies and larger corporations. [53] With respect to government agencies, this is through the implementation of 11 Information Privacy Principles, and for private sector organizations without an approved privacy code, 10 National Privacy Principles. [54]

Although broad in application, the privacy principles only regulate personal information divulged in particular circumstances. The Act also contains a number of exceptions that inhibit its ability to provide effective redress to employees. For example, information in employee records held by private companies is exempt under the Act. [55]

---

[50] Parliament of Australia - Senate Standing Committee on Legal and Constitutional Affairs, 'Telecommunications (Interception and Access) Amendment Bill 2007 [Provisions]' (August 2007), [2.2].

[51] *Privacy Act* 1988 (Cth); *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, (adopted 23 September 1980) <http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186-1-1-1-1,00.html> at 1 February 2008.

[52] *International Covenant on Civil and Political Rights*, G.A. res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171, (entered into force March 23, 1976) <http:///www1.umn.edu/humanarts/instree/b3ccpr.htm> at 1 February 2008.

[53] Section 6(1) defines personal information 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." Businesses with an annual turnover for the previous financial year of $3,000,000 or less are exempt from the Act's provisions: ss 6C(1), 6D(1).

[54] ss 14, 16A(2), sch 3.

[55] s 7B(3). For further information on exemptions see Australian Law Reform Commission, *Review of Privacy*, Issues Paper No. 31 (2006), [3.48]-[3.58].

The Act provides the Privacy Commissioner with a range of options when dealing with complaints, including the authority to award monetary compensation. [56] Determinations by the Privacy Commissioner however are neither binding nor conclusive between the parties. [57]

The *Privacy Act* in its present form is limited with respect to regulating monitoring. The legislation is the subject of a review by the Australian Law Reform Commission. [58] Adoption of some of the recommendations would provide greater protection to employees from intrusions caused by electronic monitoring.

With the exception of Western Australia, [59] all states and territories have implemented information privacy measures either legislatively or by way of administrative instrument. [60] These measures mirror to varying degrees the structure and intent of the Commonwealth statute.

Queensland has adopted a policy driven approach through Information Standard 42 ("IS42"). [61] IS42 contains a set of mandatory principles governing the collection and use of personal information by government agencies, statutory bodies, and where the Minister gives notification, statutory Government Owned Corporations. [62]

The Queensland Health standard contains principles based on the NPP's from the Commonwealth *Privacy Act*. [63] An associated standard, Information Standard 38

---

56 s 52(1).
57 s 52(1B).
58 Australian Law Reform Commission, *Review of Australian Privacy Law*, Discussion Paper No. 72 (2007). This is discussed further in Chapter Four.
59 The Information Privacy Bill 2007 was introduced into the West Australian Legislative Assembly on 28 March 2007.
60 *Privacy and Personal Information Protection Act 1998* (NSW); *Information Privacy Act 2000* (Vic); Information Standards 42, 42A (Qld); *Cabinet Administrative Instruction to comply with Information Privacy Principles* (1989, 1992) (SA); *Personal Information Protection Act 2004* (Tas); *Information Act 2002* (NT).
61 Queensland Government Chief Information Officer, Information Standard 42 <http://www.qgcio.qld.gov.au/02_infostand/standards/is42.pdf> at 1 February 2008. See also Jonathan Horton, 'The Queensland privacy scheme' [2002] PLPR 5.
62 See cl 1.1 Information Standard 42.
63 Information Standard 42A <http://www.qgcio.qld.gov.au/02_infostand/standards/is42a.pdf> at 1 February 2008.

("IS38"), aims to ensure consistency across government with respect to information and communications technology polices and procedures. [64]

Both IS42 and IS38 lack the force of legislative enforcement and only apply to information held by the public sector. In addition, they do not regulate video or other types of monitoring nor provide penalties or remedies where a breach occurs. [65]

Surveillance Regulation

New South Wales first introduced legislation to regulate covert video surveillance of employees in 1998. [66] In 2005, the Government enacted the *Workplace Surveillance Act.* More comprehensive than its predecessor, the Act regulates both overt and covert surveillance by video, computer, and tracking devices such as GPS, principally through the requirement to provide prior notice of monitoring. [67]

Victoria's *Surveillance Devices (Workplace Privacy) Act*, which commenced on 1 July 2007, regulates the intentional use of optical and listening devices in certain designated areas of the workplace including toilets and change rooms. [68] The Act also prohibits a person knowingly communicating or publishing information acquired by such devices in these locations. [69]

In 2000, Jon Stanhope introduced a private members Bill in the Australian Capital Territory Legislative Assembly to regulate video surveillance in public places. [70]

---

[64] Queensland Government Chief Information Officer, 'Use of ICT Facilities and Devices (IS38)' < http://www.qgcio.qld.gov.au/02_infostand/is38_print.pdf>; Office of the Public Service Commissioner, 'Use of Internet and Electronic Mail Policy and Principles Statement' <http://www.opsc.qld.gov.au/library/docs/resources policies/internet_and_email_policy.pdf >at 2 June 2008.

[65] In 1971 Queensland enacted the *Invasion of Privacy Act.* Although this legislation is primarily aimed at regulating listening devices, unlawful entry to a dwelling house constitutes an invasion of privacy under the Act with a maximum penalty of 20 penalty units or imprisonment for 1 year: s 48A.

[66] *Workplace Video Surveillance Act 1998.*

[67] ss 3, 10-13, Part 4.

[68] s 9B(1).

[69] s 9C(1).

[70] Surveillance Cameras (Privacy) Bill 2000 (introduced by Jon Stanhope, the Member for Ginninderra). The Bill lapsed on the 20th October 2001 (declaration of the 2001 poll).

Although the Bill focuses on public surveillance, many of the provisions are suitable for implementation in a workplace setting. The Victorian Law Reform Commission has also released a report on workplace surveillance that contains a comprehensive draft Bill. [71]

Residual Common Law Protections

In the absence of legislation, employees may be able to seek redress through an action at common law. [72] Traditionally, courts in Australia have been reluctant to recognise the existence of a common law action for invasion of privacy. [73] However, in 2001, some members of the High Court expressed the view that the decision in *Victoria Park* did not stand in the way of the development of a tort of invasion of privacy. [74] The Queensland District Court in *Grosse v Purvis* went a step further allowing the plaintiff to recover damages for breach of privacy. [75] More recently, a plaintiff victim of rape received damages for breach of privacy when a radio station broadcast identified her by name and other relevant details. [76]

There have been relatively few decisions at this stage, thus it is unclear exactly how the tort will develop in Australia. In relation to workplace privacy however, the experience in the United States indicates a privacy tort may provide only limited assistance to employees.

The United States

The New Hampshire Supreme Court issued the first published decision recognising a

---

71 Appendix 5, Victorian Law Reform Commission, *Workplace Privacy Final Report* (2005).

72 For a detailed discussion on common law actions relevant to privacy see Carolyn Doyle, Mirko Bagaric, *Privacy Law in Australia* (2005), 57-97.

73 *Victoria Park Racing and Recreation Grounds Co Limited v Taylor* (1937) 58 CLR 479. See also *Kalaba v Commonwealth of Australia* [2004] FCA 763; *Giller v Procopets* [2004] VSC 113.

74 See *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 248-9 (Gummow, and Hayne JJ), 231 (Gaudron J), 321-28, (Callinan J). Justice Murphy also referred to the developing tort of "unjustified intrusion of privacy" in *Church of Scientology Inc v Woodward* (1982) 154 CLR 25, 68.

75 *Grosse v Purvis* (2003) Aust Torts Reports ¶81-706.

76 *Doe v ABC & Ors* [2007] VCC 281.

right to privacy in 1816. [77] In 1890, Warren and Brandeis, concerned over intrusions by the press into the private lives of individuals, argued the merits of establishing a common law action for invasion of privacy. [78] Following the decision in *Roberson v. Rochester Folding Box Company*, New York created a statutory privacy tort in 1903. [79] In 1960, William Prosser (then Dean of the University of California Law School), after analysing the significant body of case law that had developed since the Warren and Brandeis article, concluded that the right to privacy "…is not one tort, but a complex of four." [80] The *Restatement of Torts*, applied extensively by courts throughout the United States, reflects Prosser's categorisation of the four cases of action - unreasonable intrusion upon the seclusion of another, appropriation of the other's name or likeness, unreasonable publicity given to the other's private life, and publicity that unreasonably places the other in a false light before the public. [81]

In parallel with these developments was the gradual recognition by the United States Supreme Court of a constitutional right to privacy. Through a number of landmark decisions, the Fourth Amendment's prohibition against unreasonable search and seizure has developed to protect individuals from unwarranted physical and electronic intrusions by government officials. [82]

The Supreme Court has also recognised a right to privacy in a number of other guarantees under the Bill of Rights. [83] In *Griswold v. Connecticut*, Mr. Justice Douglas

---

77 Charles E. Frayer, 'Employee Privacy and Internet Monitoring: Balancing Workers' Rights and Dignity with Legitimate Management Interests' (2002) 57(2) *The Business Lawyer* 857, 860 (Citing *Ward v Bartlett*).

78 Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.

79 See Daniel J. Solove, Marc Rotenberg and Paul M. Schwartz, *Information Privacy Law* (2006), 25-6. (Citing *N.Y Civ. Rights Act* § 51).

58 William L. Prosser, 'Privacy' (1960) 48(3) *California Law Review* 383, 389. For a critical analysis of Prosser's categorisation see Edward J Bloustein, above n 11.

81 *Restatement (Second) of Torts* (1977), § 652B to E. The Restatement contains an outline of principles applied plus a commentary.

82 These include *Boyd v. United States*, 116 U.S. 616 (1886); *Olmstead v. United States*, 277 U.S. 438 (1928); *Goldman v. United States*, 316 U.S. 129 (1942); *Katz v. United States*, 389 U.S. 347 (1967); *Berger v. New York*, 388 U.S. 41 (1967); *Kyllo v. United States*, 533 U.S. 27 (2001); *Smith v. Maryland*, 442 U.S. 735 (1979); *United States v. Knotts*, 460 U.S. 276 (1983). See also Ken Gormley, 'One Hundred Years of Privacy' (1992) *Wisconsin Law Review* 1335, 1357-74; Robert B. McKay, 'The Right of Privacy: Emanations and Intimations' (1965-6) 64 *Michigan Law Review* 259, 272-75.

83 *Griswold v. Connecticut* 381 U.S. 479 (1965) (Douglas J). Amendments 1 through 10 of the United States Constitution comprise the Bill of Rights.

for the Court noted that the case law discussed indicates "…specific guarantees in the *Bill of Rights* have penumbras, formed by emanations from those guarantees that help give them life and substance…" and that the "[v]arious guarantees create zones of privacy." [84]

There are also two relevant statutes at the federal level. The *Privacy Act* protects personal information held by federal government agencies. [85] The Act performs a similar function to its Australian counterpart, although it does not apply to the private sector, and is generally somewhat more restricted in its mode of operation.

The *Electronic Communications Privacy Act* ("ECPA") offers employees more comprehensive protection and scope for redress. [86] The ECPA prohibits unauthorised interceptions of wire, oral and electronic communications, and unauthorised access to stored communications, and provides for criminal sanctions, fines, and civil remedies. [87] The ECPA contains a number of exceptions however, which limit its effectiveness in protecting employees' privacy rights at work. [88]

There have been three notable attempts to introduce workplace privacy legislation at the federal level. [89] To date none of these measures has been able to attract sufficient support in Congress.

Following the Supreme Court's decision in *Katz v. United States* a number of states incorporated provisions similar to the Fourth Amendment in their constitutions. [90] Some

---

84 Ibid 484.

85 *Privacy Act of 1974*, Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C § 552a (2006)).

86 *Electronic Communications Privacy Act of 1986*, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510-2522, 2701-2712 (2006)).

87 §§ 2511(1), 2511(4), 2520, 2701, 2707.

88 For example, interceptions are lawful where one of the parties consents: § 2511(2)(c),(d), or where the employer is acting as a service provider: § 2511(2)(a)(i): see Ray Lewis, 'Employee E-mail Privacy Still Unemployed: What the United States Can Learn from the United Kingdom' (2007) 67 *Louisiana Law Review* 959, 970-3.

89 S. 984, Privacy for Consumers and Workers Act, 103d Cong., 1st Sess. (1993); H.R. 4908, Notice of Electronic Monitoring Act, 106th Cong., 2d Sess. (2000); H.R. 582, Employee Changing Room Privacy Act, 109th Cong., 1st Sess. (2005).

90 *Katz v. United States*, 389 U.S. 347 (1967). See Gormley, above n 82, 1423.

state constitutions also contain an express provision protecting general privacy rights. [91] In addition, forty-eight states have enacted measures similar to the ECPA. [92] Other state based legislation for example, includes the requirement that both parties provide consent before the implementation of email monitoring, and a prohibition on using computers to examine personal information without appropriate authority. [93] Some states, including Delaware and Connecticut, have enacted specific workplace privacy measures. [94] The common law action of invasion of privacy is also widely available at the state level. [95]

Conclusion

Electronic monitoring provides employers with unprecedented access to information about their workers. Without appropriate regulation, this has the potential to adversely affect employees' privacy rights. Current legislative and other measures in both Australia and the United States do not sufficiently address the privacy concerns raised by the increased use of sophisticated monitoring technologies in the workplace.

Analysing existing (and proposed initiatives) in both jurisdictions will assist the development of a comprehensive national legislative strategy to regulate electronic monitoring in Australian workplaces. The legislation will protect employees' privacy rights whilst providing employers with the opportunity to conduct a reasonable level of monitoring.

---

91 For example *Constitution of the State of California* art. I, § 1: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." See also Lewis, above n 88, 975.

92 Ibid.

93 Mary E. Pivec and Susan Brinkerhoff, 'E-Mail in the Workplace: Limitations on Privacy' (1999), 26(1) *Human Rights* 22, 23.

94 *Delaware Labor Code*, Title 19, § 705 (2007); *Conn. Gen. Stat.* § 31-48d (2007). Other states including Georgia, Arkansas, and Minnesota have attempted to introduce legislation.

95 For a brief history of privacy torts see Mac Cabal, 'California to the Rescue: A Contrasting View of Minimum Statutory Damages in Privacy Torts' (2007) 29 *Whittier Law Review* 273, 274-77.

Chapter Two

Overview of Privacy Protection and Issues Affecting Workplace Privacy in Australia and the United States

This chapter provides an overview of privacy law as it relates to electronic monitoring in Australia and the United States. There is also analysis of proposed workplace privacy measures from both jurisdictions.

AUSTRALIA

The Commonwealth and Australian Capital Territory

Efforts to recognise and protect privacy rights under Australian law have focused on legislative instruments. Despite an initial failed attempt through the Human Rights Bill in 1973, [1] in 1988 the Commonwealth enacted comprehensive information privacy legislation in the form of the *Privacy Act*. [2]

The Privacy Act

Overview

Through the statutory office of Privacy Commissioner, the Act regulates acts and practices involving the collection, storage, use, and disclosure of personal information by government agencies (both Commonwealth and the Australian Capital Territory), and larger private sector companies. [3]

The legislation applies to the collection and handling of information by organizations

[1] See Office of the Victorian Privacy Commissioner, 'Info Sheet 07.02 - A Brief History of Information Privacy' (19 June 2002). See generally Roger Clarke, 'A History of Privacy in Australia' (2002) <http://www.anu.edu.au/people/Roger.Clarke/DV/OzHistory.html> at 28 February 2008.

[2] *Privacy Act 1988* (Cth).

[3] See ss 6(1), 6C, 6D-EA, 7, Part IV.

where "…the information is collected for inclusion in a record or a generally available publication." [4] A record is a document, database, photograph, or other form of pictorial representation of an individual. [5]

There are 11 Information Privacy Principles (IPP's) that govern the handling of personal information by government agencies, and 10 National Privacy Principles (NPP's) performing the same function for private organizations that do not have an approved privacy code. [6] An amendment to the Act in 2000 established a single national scheme to regulate the handling of personal information by the private sector through the adoption of privacy codes and the NPP's. [7]

The IPP's impose a number of obligations on agencies, including only collecting information for a lawful purpose directly related to a function or activity of the collector, informing the individual the purpose of the collection, and allowing individuals reasonable access to records held by agencies that contain their personal information. [8] Private organizations must have an approved privacy code, or in its absence, comply with the NPP's, which provide comparable obligations to those imposed on government agencies. [9] A privacy code is a documented set of processes and procedures approved by the Privacy Commissioner regulating the acts and practices of the company that affect privacy. [10]

Exemptions

The Act contains a number of exemptions that limit its effectiveness. Two of these

4 s 16B (Tax file numbers and credit information are exempt from this requirement).
5 s 6(1). Exceptions include generally available publications, documents governed by the *Archives Act 1983* and material in transit by post.
6 ss 14, 16A(2), sch. 3.
7 s 3, *Privacy Amendment (Private Sector) Act 2000* (Cth). Obligations under a privacy code must equal or exceed those prescribed by the NPP's and be approved by the Privacy Commissioner: Attorney-General's Department and Department of Employment and Workplace Relations, 'Employee Records Privacy - A discussion paper on information privacy and employee records' (February 2004), [1.26].
8 See s 14 (Principles 1, 2 and 6).
9 s 16A(2), sch 3.
10 s 6(1), Part IIIAA.

particularly affect workplace privacy. Firstly, the Act does not regulate personal information collected by small businesses. [11] This means up to 94% of all business in Australia may be exempt from the Act's provisions. [12]

An exemption also applies to information in employee records held by the private sector. The Act defines employee records to include information relating to the employment of an individual, including terms and conditions of engagement, hours of work, performance or conduct, and financial details. [13]

The effect of the exemption is to remove the protection of the Act with respect to acts or practices engaged in by a private employer that are "…directly related to:…a current or former employment relationship between the…" parties, and that individual's employee record. [14] Thus, information acquired through monitoring in circumstances where there exists a sufficient connection between such monitoring and the employee record of the individual concerned may not attract the protection of the Act.

If there does not exist a sufficient connection to an employee's record, the monitoring activities may fall within the Act's provisions. [15] This could include where the monitoring conducted is not in proportion to the risk it was seeking to address, is done out of curiosity, captures emails which contain information about a non-employee, or emails from outside the company, or where there are no guidelines informing employees how monitoring relates to their employment. [16] The exemptions however mean a

---

[11] s 6C(1). "Organisation" does not include a small business operator, defined in s 6D(1) as a business with an annual turnover in the previous financial year of $3,000,000 or less.

[12] Australian Law Reform Commission, *Review of Australian Privacy Law*, Discussion Paper No. 72 (2007), [35.1].

[13] s 6. See generally Attorney-General's Department and Department of Employment and Workplace Relations, above n 7.

[14] s 7B(3). The exemption does not apply to information provided by job applicants unless they subsequently become employees, or to contractors or subcontractors where they are handling personal information of employees from another organization: Office of the Privacy Commissioner, 'Information Sheet 12: 2001 Coverage of and Exemptions from the Private Sector Provisions', 4.

[15] See Robin McKenzie, 'The Privacy Act, employee records and email monitoring' (PowerPoint Slides - Office of the Privacy Commissioner Presentation to a workshop hosted by Clearswift Corporation, Perth, 5 March 2003).

[16] Ibid.

substantial number of private sector employees have little or no recourse to the Act should a breach occur.

Impact of New Technology

There have been questions raised about the effectiveness of the Act in light of advances in technology. [17] This is particularly relevant to workplace privacy. For example, closed circuit television cameras (CCTV) are becoming more common in workplaces. The definition of a record includes "…a photograph or other pictorial representation of a person…." [18] Thus, CCTV footage that sufficiently identified an individual may constitute personal information. It is uncertain whether the use of live CCTV, (where the images captured are not subsequently recorded) would fall outside the protection of the Act, because of the legislation's requirement for recording information in a material form. [19]

Apart from specific monitoring tools, collection of information about Internet usage can occur in a number of other ways, including cookies, web bugs, or by requesting web pages through a browser. [20] Email messages containing an individual's name and perhaps other relevant details in the content of the message may be sufficient to meet the definition of personal information. [21] This technology also raises other issues, for instance, email sent to multiple recipients may disclose the addresses of those persons to everyone who receives the message. [22]

---

17 Australian Law Reform Commission, *Review of Privacy*, Issues Paper No. 31 (2006), [11.111]. For a discussion of technologies see [11.4]-[11.108].

18 s 6(1).

19 Parliament of Australia – Senate Legal and Constitutional References Committee, 'The Real Big Brother: Inquiry into the Privacy Act 1988' (2005), [3.19] (Citing Anna Johnston – Australian Privacy Foundation).

20 See Australian Law Reform Commission, above n 17, [11.4]-[11.16].

21 See Robin McKenzie, above n 15. Section 6 defines personal information 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."

22 Australian Law Reform Commission, above n 17, [11.111] (Citing J Partridge).

Applicability to Workplace Privacy

The *Privacy Act* focuses on regulating personal information collected by government and larger corporations and is in many respects "light tough" regulation. [23] In a case involving the alleged improper disclosure of personal information by a government department to the Ombudsman, the Privacy Commissioner noted Australian privacy law "…is not intended to provide an absolute right to privacy…" but "…is built to accommodate other public interests, including the Ombudsman's role in promoting proper administrative practice." [24] Generally, the Act may afford some protection to employees where emails or data obtained from monitoring Internet usage (or CCTV footage) contains sufficient information to meet the definition of personal information, and the collection and handling of such violates the privacy principles.

The exemptions however limit the Act's effectiveness with respect to private sector employees. The legislation also has some difficulties coping with emerging technology. Therefore, in its current form the *Privacy Act* does not provide sufficient protection to employees from unwarranted intrusions caused by the use of electronic monitoring in the workplace.

Surveillance Cameras (Privacy) Bill

An investigation in 1996 into the efficacy of surveillance cameras by the Australian Capital Territory ("ACT") Parliament's Standing Committee on Legal Affairs resulted in a number of recommendations with respect to the use of video surveillance in public places. [25] Following the ACT Government's decision to reject a recommendation to introduce privacy legislation prior to installing cameras, Jon Stanhope (the then Leader of the Opposition), introduced a private members Bill aimed at regulating the use of

[23] "Regulation which is not intrusive or prescriptive and which is cheap to administer and comply with is often described as 'light touch.' " (Victorian Law Reform Commission, *Workplace Privacy Final Report* (2005), xii).

[24] *Complaint Determination No 5 of 2004,* APrivCmr (19 April 2004), [18], [41].

[25] Australian Capital Territory, *Parliamentary Debates*, Legislative Assembly, 29 March 2000, 997 (Jon Stanhope, Leader of the Opposition).

surveillance cameras in such areas. [26]

The Surveillance Cameras (Privacy) Bill establishes a series of specific CCTV camera privacy principles, in conjunction with a surveillance camera code to govern the authorisation, management, and operation of the cameras. [27] The Bill's objectives include protecting the privacy of those individuals recorded whilst engaged in lawful activities, and limiting how the information collected is used, for example to deter and prevent crime. [28]

The Surveillance Camera Principles include provisions governing permissible surveillance purposes, authorisation, unlawful and unfair surveillance, notice, storage and security of surveillance records, and the use and disclosure of personal information in surveillance records. [29] The Model Surveillance Camera Code includes guidelines with respect to the authorisation of surveillance on behalf of other persons and the training of operators. [30] The Code also requires "reasonable measures" be taken to prevent surveillance in private areas (such as changing rooms), and provides for an independent evaluation process for all surveillance operations. [31]

Although the Bill's focus is cameras operating in public areas, (in this case Civic in Canberra), many of the principles and practices are transferable to the workplace. The Bill lapsed on the declaration of writs for the 2001 election and to date has not been re-introduced. The ACT Government is currently considering CCTV capability and exploring the need to regulate surveillance in the workplace. [32]

Australian States and Territories

The following discussion focuses on existing workplace privacy measures in New South

[26] Ibid 997-1003.
[27] See Explanatory Memoranda, Surveillance Cameras (Privacy) Bill 2000 (ACT).
[28] Ibid 2-3.
[29] Ibid sch 1.
[30] Ibid sch 2.
[31] Ibid.
[32] Email from Victor Martin (on behalf of Jon Stanhope) to James Watt, 10 May 2007.

Wales and Victoria. There is also analysis of the draft workplace privacy Bill produced by the Victorian Law Reform Commission, information privacy laws, and the tort of invasion of privacy.

Information Privacy Laws

Queensland and South Australia regulate information privacy by way of administrative instrument. [33] Both instruments only apply to the public sector and associated agencies and contain privacy principles based on the IPP's. [34]

New South Wales, Tasmania, Victoria, and the Northern Territory have enacted information privacy legislation. [35] The legislation is broadly similar in scope and operation to that of the *Privacy Act*. There are however some relevant differences, for example, the complaint process, and levels of monetary compensation. [36]

As with South Australia and Queensland these measures generally apply only to information collected by public sector agencies. [37] Thus, where monitoring captures public sector employees' personal information, they may have some redress where the agency in question fails to deal with this information in accordance with the privacy principles.

There are also a number of other privacy related statutes at the state level. These include measures related to health records, the interception of telecommunications, and listening

---

[33] Information Standards 42, 42A (Qld); *Cabinet Administrative Instruction to comply with Information Privacy Principles* (1989, 1992) (SA).

[34] *Cabinet Administrative Instruction to comply with Information Privacy Principles*, cl 2(2), Part II, Information Standard 42, cl 1.1, 3.

[35] *Privacy and Personal Information Protection Act 1998* (NSW); *Information Privacy Act 2000* (Vic); *Personal Information Protection Act 2004* (Tas); *Information Act 2002* (NT).

[36] For example in Tasmania the Ombudsman hears complaints: s 18(1) *Personal Information Protection Act 2004*, whereas in New South Wales complaints are processed by the statutory office of Privacy Commissioner: s 45(1) *Privacy and Personal Information Protection Act 1998*. The maximum monetary compensation in the Northern Territory is $60,000: s 115(4)(b*) Information Act 2002* whereas in Victoria it is $100,000: s 43(1)(a)(iii) *Information Privacy Act 2000.*

[37] There are some exceptions. For instance complaints may be made against private organizations who provide services to the Victorian Government: see ss 3 (definition of State Contract), 17(2) (Effect of outsourcing) *Information Privacy Act 2000.* A "personal information custodian" under the Tasmanian Act also includes persons and organizations that enter into contracts involving personal information: see s 3 *Personal Information Protection Act 2004.*

devices. [38]

In 2005, the Victorian Law Reform Commission released a major report on workplace privacy that includes a draft Bill. [39] The purpose of the Bill is: [40]

> (a) to provide privacy protection for workers without unduly limiting the legitimate interests of employers in the conduct of their business; and
>
> (b) to assist in giving effect to Australia's international obligations in relation to the human right of privacy recognised in Article 17 of the International Covenant on Civil and Political Rights.

The Bill regulates the surveillance of employees engaged in both work and non-work related activities. [41] The Regulator may also publish advisory codes of practice to assist employers to meet their obligations. [42] The Bill also contains a prohibition on monitoring employees in certain areas including toilets and change rooms. [43]

There is also a comprehensive complaint and conciliation mechanism. [44] Employers found in breach face both civil and criminal penalties. [45] Overall, the Bill provides a sound regulatory framework and the opportunity for aggrieved employees to seek personal remedies.

Existing Workplace Privacy Legislation

New South Wales

New South Wales was the first state to introduce specific workplace surveillance legislation in 1998. [46] This followed an inquiry held to investigate a number of

---

38 For a list of State and Territory privacy related laws see Office of the Privacy Commissioner, 'Privacy & Related Legislation in Australia' <http://www.privacy.gov.au/privacy_rights/laws/index.html> at 20 November 2007.
39 Victorian Law Reform Commission, *Workplace Privacy Final Report* (2005), Appendix 5.
40 s 1.
41 ss 8, 9.
42 s 13.
43 s 12(a).
44 Part 4 (Complaints).
45 Part 7 (Enforcement).
46 *Workplace Video Surveillance Act 1998* (NSW).

acrimonious industrial disputes involving video surveillance. [47] The Act sought to balance an employer's right to use video surveillance to investigate unlawful activities and an employee's right to privacy. [48]

In 2005, New South Wales introduced more comprehensive workplace surveillance measures. [49] The government chose to model the new Bill on the existing Act, but extended the provisions to cover other areas of electronic surveillance. [50]

The Act regulates surveillance by camera, computer, and tracking devices. [51] Employers must provide their employees with prior notice of surveillance activities. [52] There are also some additional obligations with respect to computer, camera, and tracking surveillance, including that employers establish clearly defined monitoring practices and policies. [53] The Act prohibits surveillance "…in any change room, toilet facility or shower or other bathing facility at a workplace." [54] There are also restrictions on the use and disclosure of surveillance records. [55] Surveillance not conducted in accordance with the notice and other requirements of Part 2 constitutes covert surveillance. [56]

An employer cannot conduct (or allow the conducting of) covert surveillance on any employee at work without first obtaining authorisation from a court. [57] Proceedings

---

47 New South Wales, *Parliamentary Debates*, Legislative Assembly, 29 March 2000, 16986 (Henry Tsang, Parliamentary Secretary). See also Julian Sempill, 'Under the Lens: Electronic Workplace Surveillance' (2001) 14 *Australian Journal of Labor Law* 1, 1-2; Anna Johnston and Myra Cheng, 'Electronic Workplace Surveillance, Part 2: responses to electronic workplace surveillance – resistance and regulation' [2003] PLPR 7.

48 New South Wales, *Parliamentary Debates*, Legislative Assembly, 23 June 1998, 16253 (Paul Whelan, Minister for Police).

49 *Workplace Surveillance Act 2005.*

50 New South Wales, *Parliamentary Debates*, Legislative Assembly, 29 March 2000, 16986 (Henry Tsang, Parliamentary Secretary). Section 30 of the *Workplace Video Surveillance Act* stipulated a review of its effectiveness occur after five years from the date of assent. The decision to model the new Act on existing legislation followed a statutory review in 2003 where submissions from employer and union groups did not identify any significant deficiencies.

51 s 3.

52 s 10.

53 ss 11-13.

54 s 15.

55 s 18.

56 s 3.

57 Part 4. Exemptions include actions by law enforcement officers and monitoring under the *Casino Control Act 1992.*

against employers who breach the Act can be instigated by consent from the Minister, an officer prescribed under the regulations, the secretary of an industrial union, or by the employee subject of the surveillance. [58]

The draft Bill was criticised for not going far enough to protect employees leaving "…a significant potential for workplace surveillance to be abused, to undermine relationships between employers and employees and to invade worker privacy and dignity." [59] Others saw the legislation as unnecessary and costly for business, or believed that a system of self-regulation would be more appropriate. [60] Although noting the Bill contains "several key deficiencies", the Australian Privacy Foundation said it still represented "…a step forward in terms of tackling the issue of employee privacy,…." [61]

There is also the issue of possible inconsistency with some Commonwealth legislation with respect to how the Act may apply to Australian Government agencies. [62] The definition of interception in the *Telecommunications (Interception and Access) Act 1979* ("the TI Act") is narrower than that of computer surveillance in the *Workplace Surveillance Act* meaning, "…there is an issue regarding the extent to which the TI Act excludes the operation of the NSW Act in relation to computer surveillance." [63]

Similarly, even though the *Public Service Act 1999* (Cth) authorises the monitoring of Commonwealth Government employees' use of email and the Internet, it is unclear whether this is in accordance with, or to the exclusion of, state and territory laws. [64] There is also the question of whether the Act applies outside New South Wales, that is,

---

58 s 46(1)(a)-(d).
59 Alison Cripps, 'Workplace Surveillance' (2004), New South Wales Council for Civil Liberties, 14.
60 Lenny Roth, 'Workplace Surveillance - Briefing Paper No. 13/04' New South Wales Parliamentary Library Research Service (2004), 54, 57 (Citing submissions by the NSW State Chamber of Commerce and the Australian Retailers Association).
61 See Australian Privacy Foundation, 'Analysis of the Workplace Surveillance Bill 2005' (16 May 2005) <http://www.privacy.org.au/papers/NSWWPSurvBillAn050516.pdf>, 1.
62 Andrew Schatz and Graeme Hill, 'The extended reach of the Workplace Surveillance Act' Australian Government Solicitor, Commercial Notes No. 17 (5 October 2005), 3.
63 Ibid.
64 Ibid.

for instance, to Commonwealth employees whose usual workplace is outside New South Wales but who are seconded to work in New South Wales (or the contrary). [65]

The main concern however, is that the Act regulates principally through the provision of notice, and does not limit the extent of surveillance that can occur. The legislation also does not provide employees with personal remedies where a breach occurs.

Victoria

In 2007 Victoria enacted legislation governing the use of surveillance devices in designated areas of the workplace. [66] The legislation amends the *Surveillance Devices Act 1999* in order to enhance the applicability of its provisions to the workplace. [67] Under the Act, it is an offence for an employer to "…knowingly install, use or maintain an optical surveillance device or a listening device to observe, listen to, record or monitor the activities or conversations of a worker in a toilet, washroom, change room or lactation room in the workplace." [68]

The *Surveillance Devices Act 1999* (Vic) defines an optical surveillance device as "… any device capable of being used to record visually or observe a private activity,…." [69] A listening device is "…any device capable of being used to overhear, record, monitor or listen to a private conversation or words spoken to or by any person in private conversation,…." [70]

The *Surveillance Devices (Workplace Privacy) Act* also prohibits the knowing communication or publication of a record or report of activities or conversations obtained unlawfully using optical surveillance or listening devices. [71] Contravention of the Act (in the case of a natural person) can lead to imprisonment for up to 2 years or

[65] Ibid 4.
[66] *Surveillance Devices (Workplace Privacy) Act (2006).* The Act came into force on 1 July 2007.
[67] s 1.
[68] s 9B(1).
[69] s 3(1).
[70] s 3(1).
[71] s 9C(1).

240 penalty units or both, or in any other case a fine of 1200 penalty units. [72]

A limitation is that the Act only applies to certain devices operating in specified non-production areas of the workplace. In addition, an exemption applies where surveillance is required in these areas in accordance with the *Liquor Control Reform Act 1998*. [73]

Tort of Invasion of Privacy

Recent developments at common law may provide an additional (although at this stage limited) means of redress for workplace intrusions. In 1937, a case involving the unauthorised broadcasting of horse racing led the High Court to conclude that existing authority did not support the recognition of a common law right to privacy. [74] In 2001 the Court had an opportunity to revisit this issue. [75]

Lenah Game Meats involved an application by the operators of an abattoir for an interlocutory injunction to prevent the broadcasting of video footage of slaughtering activities at their premises. [76] Unknown trespasser(s) installed cameras at the abattoir and provided footage recorded there to an animal liberation organization that subsequently passed it on to the ABC. [77] Some members of the Court discussed the tort of invasion of privacy, expressing the view that the decision in *Victoria Park* did not stand in the way of the development of such in Australia. [78] The judgments of a majority of the Court in *Lenah* appear to indicate, "…that any development of the tort of privacy would be based on the nature of the information considered private as distinct from the manner in which that information was obtained." [79]

---

72 ss 9B(1), 9C(1). The value of a penalty unit is published each year by the Treasurer in accordance with process outlined in section 5 of the *Monetary Units Act 2004*. The value of a penalty unit in 2007-08 is $110.12.

73 ss 9B(2)(c), 9C(2)(c).

74 *Victoria Park Racing and Recreation Grounds Co Limited v Taylor* (1937) 58 CLR 479.

75 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199.

76 Ibid 214 (Gleeson CJ).

77 Ibid 215 (Gleeson CJ), 291-93 (Callinan J).

78 Ibid 248-9 (Gummow, and Hayne JJ), 231 (Gaudron J), 321-28, (Callinan J).

79 Daniel Stewart, 'Protecting Privacy, Property, and Possums: Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd' (2002) 30 *Federal Law Review* 177, 189.

The Queensland District Court in *Grosse v Purvis* went a step further allowing the plaintiff to recover damages for invasion of privacy. [80] The Court found the defendant's conduct amounted to unlawful stalking and as such involved an invasion of the plaintiff's privacy. [81]

In *Doe v ABC* the Court awarded the plaintiff damages where "…the defendants breached the plaintiff's privacy by the unjustified publication of personal information,…." [82] Her Honour Judge Hampel noted, " [t]here will always be a tension between determining rights by reference to a developing cause of action, and declining to do so because no other court has yet done so. If the mere fact that a court has not yet applied the developing jurisprudence to the facts of a particular case operates as a bar to its recognition, the capacity of the common law to develop new causes of action, or to adapt existing ones to contemporary values or circumstances is stultified." [83]

These decisions indicate that it may be possible for an employee to consider an action in tort for invasion of privacy at work. However, until there is a decision dealing specifically with a breach in the workplace, or the appellate courts consider the issues raised by existing decisions, it is difficult to determine whether the common law will offer employees an effective alternative avenue for redress.

The United States

For all its myriad manifestations and elusiveness of definition, modern privacy law owes much of its origin to concerns expressed by Warren and Brandeis in the late nineteenth century over advancements in technology allowing the press to intrude further into peoples' private lives. [84] However, concern over individual privacy emerged before publication of the Warren and Brandeis article.

---

80 *Grosse v Purvis* (2003) Aust Torts Reports ¶81-706, [483] (Skoien SJ).

81 Ibid [420]. For a detailed discussion of this case and other aspects of the development of an common action for invasion of privacy see Des Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339.

82 *Doe v ABC & Ors* [2007] VCC 281, [164] (Hampel J).

83 Ibid [161].

84 Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.

In 1888, Judge Thomas M. Cooley defined privacy as " 'the right to be let alone'. " [85] Later, E. L. Godkin (editor of "The Nation") penned an article in *Scribner's Magazine* in support of laws to protect an interest in good reputation. [86] Thus, although the belief in a right to privacy, and concern over intrusions by the press, did not originate with Warren and Brandeis, "…they were the first legal scholars to synthesize a specific legal right and to propose a tort remedy for invasion of that right." [87] From these origins, privacy sprouted like a "strawberry geranium" manifesting into the diverse forms we know today. [88] These include Fourth Amendment privacy, federal and state statutes, and the common law. A discussion of these forms follows below.

Fourth Amendment Privacy

The United States Constitution does not contain an express right to privacy. Over a number of years however, the courts have read such right into various guarantees, the most relevant in relation to electronic monitoring, being the Fourth Amendment's prohibition against unreasonable search and seizure. [89]

"The overriding function of the *Fourth Amendment* is to protect personal privacy and dignity against unwarranted intrusion by the State." [90] Although most often associated with actions by federal government agents, the Fourth Amendment prohibits unreasonable searches and seizures by state government officials through the application

---

85 James H. Barron, 'Warren and Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890): Demystifying a Landmark Citation' (1979) 13(4) *Suffolk University Law Review* 875, 886 (Citing Judge Thomas Cooley). Judge Cooley used this phrase as a working definition.

86 Ibid (Citing E.L. Godkin).

87 Ibid 884. See pages 884-88 for discussion of privacy law prior to Warren and Brandeis. See also Adam J Tutaj, 'Intrusion Upon Seclusion: Bringing an "Otherwise" Valid Cause of Action into the 21st Century' (1999) 82 *Marquette Law Review* 665, 667-70 (Discusses the landmark case of *DeMay v. Roberts*).

88 "This offshoot of the plant having blossomed, the right to privacy – like a strawberry geranium-continued to creep." (Ken Gormley, 'One Hundred Years of Privacy' (1992) *Wisconsin Law Review* 1335, 1357).

89 "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." (U.S. Const. Amend. IV).

90 *Schmerber v. California*, 384 U.S. 757, 767 (1966) (Brennan J).

of the Due Process Clause of the Fourteenth Amendment. [91]

The Fourth Amendment owes it origins to the colonial practice of empowering revenue officers (through the issuing of writs of assistance) to search for and seize smuggled goods. [92] In 1761, former Advocate-General James Otis (who resigned his office when asked to defend the legality of the writs) famously denounced the practice before the Massachusetts Superior Court. [93] Otis argued that the writs were "…the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law that ever was found in an English law-book." [94]

With a few limited exceptions, the Fourth amendment requires the issue of a warrant based on probable cause before the conduct of a search. [95] Probable cause is a judicial construct requiring an applicant for a warrant to present sufficient facts to enable a judicial officer to determine whether probable cause exists. [96] Courts have held warrantless searches unlawful even where probable cause is not in question. [97] However, "…[t]he fundamental command of the Fourth Amendment is that searches and seizures be reasonable, …." [98]

---

[91] "…nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws." (U.S. Const. Amend. XIV § 1). See also *New Jersey v T.L.O*, 469 U.S. 325, 334 (1985) (White J); *Mapp v. Ohio*, 367 U.S. 643, 655 (1961) (Clark J).

[92] *Boyd v. United States*, 116 U.S. 616, 625 (1886) (Bradley J).

[93] James Otis, 'Against Writs of Assistance' (Notes and Speech delivered before the Massachusetts Superior Court February 24, 1761) <http://www.constitution.org/bor/otis_against_writs.htm> at 14 July 2006.

[94] Ibid. See also Louis Fisher, 'Congress' Role and Responsibility in the Federal Balance of Power: Congress and the Fourth Amendment' (1986) 21 *Georgia Law Review* 107, 108-112; Silas J. Wasserstrom and Louis Michael Seidman, 'The Fourth Amendment as Constitutional Theory' (1988) 77 *Georgetown Law Journal* 19, 54-7 (where the authors discuss economic and political factors which influenced opposition to the writs).

[95] "Only in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable, is a court entitled to substitute its balancing of interests for that of the Framers." *New Jersey v T.L.O*, 469 U.S. 325, 351 (1985) (Blackmun J, concur.)

[96] See United States Government Printing Office, 'Amendment 4 – Search and Seizure' <http.www.gpoaccess.gov/constitution/pdf2002/022.pdf>, 1301-4 at 20 March 2008. It has been held that "[t]he substance of all the definitions is a reasonable ground for belief of guilt." *McCarthy v. De Armit*, 99 Pa. 63, 69 (1881) (Trunkey J).

[97] *Katz v. United States*, 389 U.S. 347, 357 (1967) (Stewart J) (Citing *Agnello v.United States*).

[98] *New Jersey v T.L.O*, 469 U.S. 325, 340 (White J).

The legal focus of the guarantee is " '…the right to be let alone, with respect to government searches and seizures which invade a sphere of individual solitude deemed reasonable by society.' " [99] This is particularly relevant with respect to searches of the interior of the home where "…there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*." [100]

Boyd v. United States was the first decision to enunciate a link between privacy and the Fourth Amendment. [101] The Court held the "…compulsory production of a man's private papers to establish a criminal charge against him, or to forfeit his property, is within the scope of the Fourth Amendment…." [102] In so doing, the Court referred extensively to Lord Camden's judgment from *Entick v Carrington* stating these principles " …affect the very essence of constitutional liberty and security." [103] Further such principles extended "…to all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life." [104]

Fourth Amendment protection in *Boyd* focussed on physical trespass and the unlawful seizure of tangible goods (in this instance thirty-five cases of plate glass seized by customs). [105] However in 1928, in his landmark dissenting judgment in *Olmstead*, the now Mr Justice Brandeis argued that Fourth Amendment protection should not be so constrained. [106] Justice Brandeis pointed out that the framers of the Constitution had "…sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations." [107] Further, "[t]hey conferred, as against the Government, the right to be let alone ..." and "[t]o protect that right, every unjustifiable intrusion by the Government

---

[99] Gormley, above n 88, 1374.
[100] *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (Scalia J).
[101] *Boyd v. United States*, 116 U.S. 616 (1886) (Bradley J).
[102] Ibid 622.
[103] Ibid 630.
[104] Ibid. See also Gormley, above n 88, 1359 where he notes Judge Cooley had previously made this link between a person's home being their castle and the Fourth Amendment.
[105] Ibid 617.
[106] *Olmstead v. United States*, 277 U.S. 438 (1928). The case involved tapping the telephones of a number of individuals suspected of violating prohibition.
[107] Ibid 478.

upon the privacy of the individual, whatever the means employed, must be deemed a violation of the *Fourth Amendment*." [108]

The majority in *Olmstead* found no violation of the Fourth Amendment because there was no actual search of a person, physical trespass, or seizure of papers or tangible effects. [109] The Court continued to follow this reasoning in a number of leading cases over the next few years. For instance in *Goldman v. United States* (decided in 1942), federal agents accessed the office of one of the petitioners (Shulman) at night and installed a listening device in the partition wall. [110] They intended to use the adjoining office to listen to what transpired at a meeting between Shulman and others taking place the following day. [111]

The device failed to work and the agents decided to use a detectaphone placed against the partitioned wall to pick up and amplify sound waves coming from Schulman's office. [112] This allowed the agents to overhear conversations in the office and telephone calls made by Schulman. [113] In refusing to overrule or distinguish the decision in *Olmstead,* the Court found no violation of the Fourth Amendment because "…the trespass did not aid materially in the use of the detectaphone." [114]

In 1961 in *Silverman v. United States,* agents drove a "spike mike" under the boards of a vacant house into the party wall of the adjoining property occupied by the petitioner. [115] The spike struck the heating duct of the petitioner's house, thus converting the heating system into a conductor of sound allowing the agents to overhear conversations throughout the house. [116] The Court held that as the spike mike made contact with the heating system, this constituted a physical intrusion into the petitioner's home in

[108] Ibid. See also Gormley, above n 88, 1360-2.
[109] Ibid 466 (Taft CJ).
[110] *Goldman v. United States*, 316 U.S. 129, 131 (1942) (Roberts J).
[111] Ibid.
[112] Ibid.
[113] Ibid 131-2.
[114] Ibid 135.
[115] *Silverman v. United States*, 365 U.S. 505, 506 (1961) (Stewart J). A spike mike is a microphone, amplifier and earphones attached to a spike approximately one foot long.
[116] Ibid 506-7.

violation of the Fourth Amendment. [117] However, in *Berger v. New York* (which involved the use of a recording device in an attorney's office), the Court held that decisions subsequent to *Olmstead* supported the view that the recording of conversations came within the protection of the Fourth Amendment, and the use of electronic devices to capture conversations constituted a search. [118]

In *Katz v. United States*, the Court found "the reach" of the Fourth Amendment "…cannot turn upon the presence or absence of a physical intrusion into any given enclosure." [119] Further, "…the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling." [120]

The petitioner in *Katz* violated a federal statute by placing bets from a public telephone booth. [121] Federal agents had attached a listening and recording device to the outside of the phone booth. [122] The Court of Appeals rejected the argument that the agents' actions were in violation of the Fourth Amendment because there had been no physical entry of the phone booth. [123]

Before the Supreme Court Justice Stewart, (delivering the opinion of the Court), explained that the Fourth Amendment is not a general right to privacy, but protects individuals against certain kinds of government interference. [124] The scope of Fourth Amendment protection however is wider than this, but such protections often have no connection with the right to privacy. [125] Consideration of whether a given location such as a phone booth is an area protected by the Constitution is unnecessary because "…the Fourth Amendment protects people, not places." [126]

---

[117] Ibid 509-12.
[118] *Berger v. New York*, 388 U.S. 41, 51 (1967) (Clark J).
[119] *Katz v.United States*, 389 U.S. 347, 353 (1967) (Stewart J).
[120] Ibid.
[121] Ibid 348.
[122] Ibid.
[123] Ibid 348-9.
[124] Ibid 350.
[125] Ibid. Also see fn 4 (citing *Griswold v. Connecticut*).
[126] Ibid 351.

Further "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." [127] In contrast, anything an individual seeks to keep "…private, even in an area accessible to the public, may be constitutionally protected." [128]

Even though here the federal agents had acted with restraint, they had not sought court authorisation before conducting the search. [129] "These considerations do not vanish when the search in question is transferred from the setting of a home, an office, or a hotel room to that of a telephone booth." [130] Thus regardless of location a person should know they "…will remain free from unreasonable searches and seizures." [131]

In a concurring judgment, Justice Harlan, although accepting that the Fourth Amendment protected "people not places" examined the scope of such protection, which as was the case here generally required "…reference to a 'place'. " [132] His Honour added that prior decisions suggest the following test: "…first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' " [133]

The objective element of the *Katz* test has been criticised for being "…circular, and hence subjective and unpredictable." [134] Some have argued it provides "...an insufficient guarantee against invasions of privacy because the Amendment's protections are

---

[127] Ibid. This is commonly referred to as the 'knowing exposure" exception.
[128] Ibid.
[129] Ibid 356.
[130] Ibid 359.
[131] Ibid. The surveillance led to the petitioners conviction thus the agents had violated his Fourth Amendment rights.
[132] Ibid 361 (Harlan J).
[133] Ibid.
[134] *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (Scalia J) (and references therein). However, his Honour pointed to the decision in *Rakas* where Rehnquist J states amongst other things "… a 'legitimate' expectation of privacy by definition means more than a subjective expectation of not being discovered." (Using the example of a burglar having a justifiable subjective expectation of privacy in the house they are robbing but that such is not one the law would recognise as legitimate or society as reasonable). Further, that "[l]egitimation of expectations of privacy by law must have a source outside of the *Fourth Amendment*, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society." *Rakas v. Illinois* 439 U.S. 128, 143-4 (1978), fn 12.

apparently made contingent on the very government practices the Amendment is supposed to regulate." [135] Others have described it as "…both results-driven and malleable." [136]

Nonetheless, *Katz* remains the standard applied by courts when evaluating the reasonableness of searches conducted by the government. Thus, a person may seek protection under the Fourth Amendment regardless of location, or whether the intrusion occurs purely by electronic means. The test applied involves considering whether an individual has a subjective expectation of privacy, and if so, whether such expectation is one society considers reasonable.

The leading decision with respect to applying the Fourth Amendment in the workplace is *O'Connor v. Ortega.* [137] For seventeen years, Dr Ortega was a psychiatrist, physician, and Chief of Professional Education at Napa State Hospital. [138] The Executive Director (Dr O'Connor) and other Hospital officials "…became concerned about possible improprieties in Dr. Ortega's management of the residency program." [139] Dr O'Connor requested Ortega take paid administrative leave to allow the Hospital time to investigate the matters. [140] Dr Ortega remained on leave (initially annual then administrative leave) until some months later when the Hospital terminated his employment. [141]

While Dr Ortega was on administrative leave, the investigation team conducted a number of searches of his office. [142] They seized both hospital and personal property "…including a Valentines Day card, a photograph, and a book of poetry…." [143] The initial justification for the search was that Hospital policy required the performance of

[135] Sam Kamin, 'The Private Is Public: The Relevance of Private Actors in Defining the Fourth Amendment' (2004) 46 *Boston College Law Review* 83, 96-7 (and references cited therein).
[136] Ibid 97.
[137] 480 U.S. 709 (1987).
[138] Ibid 712 (O'Connor J).
[139] Ibid. The allegations involved Dr Ortega's acquisition of a computer, allegations of sexual harassment by two female employees, and inappropriate disciplinary action against a resident.
[140] Ibid.
[141] Ibid 712-3.
[142] Ibid 713.
[143] Ibid.

"…a routine inventory of state property in the office of a terminated employee." [144] Dr Ortega maintained the search was to gather evidence to use against him in disciplinary proceedings, and that the hospital violated his Fourth Amendment rights through allowing the investigation team to conduct the search. [145]

Five members of the Court concluded Dr Ortega had a reasonable expectation of privacy in his office. [146] All members of the Court held he enjoyed a similar expectation with respect to his desk and filing cabinets. [147] However, opinion differed on how such expectation should be determined.

Four members of the majority held that although an individual does not lose their entitlement to Fourth Amendment protection because they work for the government, "…operational realities of the workplace, however, may make *some* employees' expectations of privacy unreasonable when an intrusion is by a supervisor rather than a law enforcement official." [148] Further an "…employee's expectation of privacy must be assessed in the context of the employment relation." [149]

The nature of government offices means a range of people (including supervisors and other employees) may frequently access an individual's office and "…some government offices may be so open to fellow employees or the public that no expectation of privacy is reasonable." [150] Thus, given such diversity in public sector work environments "… the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis." [151] The same four members of the Court also held that requiring an employer to obtain a warrant before entering an employee's office (or their desk and filing cabinets) for work related purposes "…would seriously disrupt the

[144] Ibid. At the time Dr Ortega was still on administrative leave.
[145] Ibid 713-4.
[146] Ibid 731-2 (Scalia J, concur), 732 (Blackmun, Brennan, Marshall, Stevens JJ, diss).
[147] Ibid 719 (O'Connor J, Rehnquist CJ, White, Powell JJ), 731-2 (Scalia J, concur), 732 (Blackmun, Brennan, Marshall, Stevens JJ, diss).
[148] Ibid 717 (O'Connor J, Rehnquist C J, White, Powell JJ).
[149] Ibid.
[150] Ibid 717-8.
[151] Ibid 718.

routine conduct of business and would be unduly burdensome." [152] Similarly, requiring probable cause for such searches "…would impose intolerable burdens on public employers." [153] Instead, ascertaining the reasonableness of searches by government employers involved balancing "…the invasion of the employees' legitimate expectations of privacy against the government's need for supervision, control, and the efficient operation of the workplace." [154]

Justice Scalia delivered a concurring judgment but disagreed on the reason for reversal and the standard prescribed for searches. [155] His Honour questioned how accessible an office had to be before it is considered "so open" that no expectation of privacy is reasonable, and how police are to gather the facts necessary to determine such. [156] There was also concern that a case-by-case approach would produce rather than eliminate uncertainty. [157] In addition, the proposed standard must be incorrect if on the facts it means Dr Ortega has no protection under the Fourth Amendment where the investigative team had sufficient work-related reasons for entering his office. [158] "It is privacy that is protected by the Fourth Amendment, not solitude." [159]

His Honour also disagreed with the contention that some employees may not have a reasonable expectation of privacy where the intrusion is by their supervisor instead of a law enforcement official. [160] However, "…government searches to retrieve work-related materials or to investigate violations of workplace rules...that are regarded as reasonable and normal in the private-employer context - do not violate the Fourth Amendment." [161]

---

[152] Ibid 722 (O'Connor J, Rehnquist C J, White, Powell JJ).
[153] Ibid 724.
[154] Ibid 719-20.
[155] Ibid 729 (Scalia J).
[156] Ibid 729-30 (Scalia J).
[157] Ibid 730.
[158] Ibid. O'Connor J, Rehnquist CJ, White, Powell JJ held that the Court of Appeals should have remanded the case back to the District Court because the record did "…not reveal the extent to which Hospital officials may have had work-related reasons to enter Dr Ortega's office,…." (718).
[159] Ibid. Justice Scalia noted that just as an individual has an expectation of privacy at home even though others have access (including family members and the landlord who can conduct unannounced inspections at any time), a person's office "… is constitutionally protected against warrantless intrusions by the police, even though employer and co-workers are not excluded."
[160] Ibid 731. See O'Connor J, Rehnquist CJ, White, Powell JJ (717).
[161] Ibid 732.

Justice Blackmun writing for the dissenting members in holding the search violated Dr Ortega's Fourth Amendment rights, criticized the abandonment of the warrant-probable cause requirement and its replacement by a balancing test for ascertaining the standard of reasonableness. [162] Thus, "…only when the practical realities of a particular situation suggest that a government official cannot obtain a warrant based upon probable cause without sacrificing the ultimate goals to which a search would contribute, does the Court turn to a 'balancing' test to formulate a standard of reasonableness for this context." [163]

The *O'Connor* standard means Fourth amendment protection extends to searches and seizures of government employees' private property. The court must determine if an employee has a subjective expectation of privacy, and whether it is one society considers reasonable. Evaluation of whether an employee has a reasonable expectation of privacy in any given circumstance is on a case-by-case basis. What is reasonable depends on the context, and involves balancing an employee's legitimate expectation of privacy against the operational realities of the workplace.

Evolving technology has influenced Fourth Amendment analysis through the creation of novel methods for conducting searches. For example in *Kyllo*, a federal agent used a thermal imaging device to determine the amount of heat emanating from the petitioner's home. [164]

Justice Scalia for the Court stated "[i]t would be foolish to contend that the degree of privacy secured to citizens by the *Fourth Amendment* has been entirely unaffected by the advance of technology." [165] "The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy." [166]

---

[162] Ibid 732-3 (Blackmun, Brennan, Marshall and Stevens JJ).

[163] Ibid 741. Justice Blackmun further suggested the Court "…examine closely the practical realities of a particular situation and the interests implicated there before replacing the traditional warrant and probable-cause requirements with some other standard of reasonableness derived from a balancing test." (748).

[164] *Kyllo v United States*, 533 U.S. 27, 29-30 (2001) (Scalia, Souter, Thomas, Ginsburg, Breyer, JJ). The agent believed Kyllo was growing marijuana in the house and hoped the device would indicate heat emanating from lamps used on the plants.

[165] Ibid 33-4.

[166] Ibid 34.

His Honour proposed that "[w]here, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." [167] *Kyllo* illustrates the challenges technology poses for personal privacy, and reinforces the importance of the Fourth Amendment's role in protecting privacy in the home.

Apart from the focus on the home, another limitation of the Fourth Amendment is that it only applies to public sector employees. There is also the difficulty in applying the case law (much of which relates to alleged criminal acts) to actions in the workplace. Although the Fourth Amendment is a significant bulwark against intrusions of an individual's privacy by government, unfortunately, historical and other limitations diminish its ability to protect employees from intrusions caused by electronic monitoring.

Federal Legislation

The United States does not have a national privacy agency, although there have been attempts to create one. [168] However, the *Homeland Security Act of 2002* allows for the appointment of a senior official with responsibility for privacy policy. [169]

There are two major statutes at the federal level relevant to privacy. The *Privacy Act* regulates information supplied to government agencies, [170] while the *Electronic Communications Privacy Act* (ECPA) prohibits the unlawful interception of, or access to, wire, oral and electronic communications. [171]

---

[167] Ibid 40. Casey Holland refers to this as the "Kyllo General-Public-Use Test." See Casey Holland, 'Neither Big Brother Nor Dead Brother: The Need for a New Fourth Amendment Standard Applying to Emerging Technologies' (2005-6) 94 *Kentucky Law Journal* 393, 399-401.

[168] See Robert Gellman, 'A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board' (2002-3) 54 *Hastings Law Journal* 1183, 1192-97.

[169] Ibid 1189.

[170] *Privacy Act of 1974*, Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C § 552a (2006)).

[171] *Electronic Communications Privacy Act of 1986*, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510-2522, 2701-2712 (2006)).

The Privacy Act

In 1972, a committee headed by the then Secretary of Health, Education and Welfare was formed to address concerns "…about the harm that could result from the unfettered use of computer and telecommunications technology to collect, store and use data about individual citizens." [172] The Committee's report outlined five fair information privacy principles that later formed part of the *Privacy Act.* [173] The emergence of the legislation reflects a number of concerns raised at the time including "…the inherent dangers of the growing ease of electronic surveillance capabilities and the vast amount of information gathered about individuals in computer data banks." [174]

The Act regulates records containing information on individuals held by government agencies. An agency is an "…authority of the Government of the United States, whether or not it is within or subject to review by another agency…." [175] Agencies include military departments and government corporations, however, a number of entities are excluded, including Congress, the courts, the government of the District of Columbia, and the governments of territories or possessions of the United States. [176]

A record is: [177]

> any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph;

Agencies must hold information in a "system of records" which is: [178]

---

[172] Oliver Ireland and Rachel Howell, 'The Fear Factor: Privacy, Fear and the Changing Hegemony of the American People and the Right to Privacy' (2003-4) 29 *North Carolina Journal of International Law and Commercial Regulation* 671, 674.

[173] Ibid.

[174] Haeji Hong, 'Dismantling the Private Enforcement of the Privacy Act of 1974: Doe v. Chao' (2005) 38 *Akron Law Review* 71, 80-1 (Citing remarks by Sen. Jackson). For discussion of the congressional debates, history and overview of the Act see pages 80-93.

[175] See §§ 552a(a)(1), 552(f)(1), 551(1) Agency is defined by cross-reference to the *Freedom of Information Act* (contained in § 552).

[176] §§ 552(f)(1), 551(1)(A)-(H).

[177] § 552a(a)(4).

[178] § 552a(a)(5).

> a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual;

Maintaining records includes maintaining, collecting, using and disseminating information. [179]

The Act contains a number of principles that govern the handling of the data contained in a system of records. These include only holding information necessary to accomplish the agency purpose(s), providing notice about the authority to collect, the routine uses that may be made of the information, and maintaining records used in making determinations in a manner that ensures fairness to the individual concerned. [180] Agencies also have a number of obligations with respect to providing individuals with access to their records. [181]

Civil remedies are available where an agency breaches its obligations under the Act. [182] Where an agency fails to appropriately maintain an individual's record, or commits any other breach of the section, such breach having an adverse effect on the individual concerned, and it is shown the agency acted intentionally or wilfully, an individual may recover actual damages sustained (minimum $1,000) plus litigation costs including reasonable attorney fees. [183] To qualify for the minimum statutory award however, a plaintiff must show they have suffered actual damage. [184]

The legislative history of the Act indicates that general damages are not available. [185] There also exist conflicting opinions with respect to whether the actual damage requirement permits only recovery for pecuniary loss, or encompasses conditions such as mental injury. [186]

---

[179] § 552a(a)(3).
[180] § 552a(e).
[181] § 552a(d).
[182] § 552a(g).
[183] §§ 552a(g)(1)(C),(D), 552a(g)(4).
[184] *Doe v. Chao*, 540 U.S. 614, 627 (2004) (Souter J).
[185] Ibid 622-3.
[186] Ibid 627 (fn. 12) citing *Fitzpatrick v. IRS* (pecuniary loss only), *Johnson v Department of Treasury* (can include mental anxiety).

Criminal penalties are also possible. For instance, an officer or employee of an agency who unlawfully and wilfully discloses information about an individual in contravention of the Act, or who maintains a system of records without meeting the notice requirements is guilty of a misdemeanour and subject to a fine up to $5000. [187] The same penalty applies where a person obtains information from an agency under false pretences. [188] The court can also order the agency to amend an individual's record in accordance with their request, or produce records deemed improperly withheld. [189]

The Act contains a number of exceptions that can limit its effectiveness. For example, an agency may disclose a person's record without requiring their prior written consent where such is compatible with the purpose for collection. [190] Similarly, consent is not required if the disclosure involves a request under the *Freedom of Information Act*, [191] or involves sharing the data with another agency for a civil or criminal law enforcement activity. [192]

In addition, the system of records requirement means it is not sufficient that an agency has a capability of retrieving records by name, individual identifier or similar, it must actually do so. [193] Also, unlike the *Freedom of Information Act*, an individual cannot request access to records that may contain relevant information, but only such information that is held by the agency in a system of records. [194] This means even where an agency may hold relevant information about an individual (perhaps acquired through monitoring), it may not be possible for that individual to access such if the data is not held in accordance with the requirements of the Act.

Another issue is the impact of changing technology. The system of records requirement "…involves examining the actual retrieval methods used by an agency to determine if

[187] § 552a(i)(1),(2).
[188] § 552a(i)(3).
[189] § 552a(g)(2)(A),(3)(A).
[190] §§ 552a(b)(3), 552a(a)(7). Referred to as the routine use exemption.
[191] § 552a(b)(2).
[192] § 552a(b)(7).
[193] *Henke v. United States*, 83 F.3d 1453, 1460-1 (DC. Cir. 1996) (Wald J).
[194] Fred R. McCarroll (DOE/OHA, 1/26/07) Case No. TFA-0186, 2. "Nevertheless, the standard of sufficiency that we demand of a PA search is no less rigorous than that of a FOIA search."

the records fit into the definition,…." [195] However current technology makes searching electronic information easier, meaning agencies can search for records using "…virtually any word or number contained in their systems." [196] The question is then how many times an agency must perform a retrieval using a person's name to produce a system of records. [197]

The requirement to demonstrate actual damage may also limit the ability of a plaintiff to seek effective redress. Even though in *Doe v. Chao* the government conceded disclosure of the plaintiff's social security number in contravention of the Act, no remedy was available because Doe had not produced sufficient corroborating evidence of his claim for emotional distress. [198]

The definition of agency in the Act is reasonably extensive. However, unlike Australia, the Act does not apply to the private sector. The Supreme Court is yet to determine whether to extend constitutional protection to information privacy, however has acknowledged that there may be privacy rights attached to personal information. [199] Absent such, recourse for many public sector employees may be through the *Privacy Act*. Unfortunately, given the nature of the legislation and the limitations discussed above, the Act is not the most suitable avenue for an employee seeking redress for a breach of their privacy caused by electronic monitoring.

Electronic Communications Privacy Act

The *Electronic Communications Privacy Act of 1986* ("ECPA") amended Title III of the *Omnibus Crime Control and Safe Streets Act* (commonly know as the *Federal Wiretap*

[195] Julianne M. Sullivan, 'Will the Privacy Act of 1974 Still Hold up in 2004? How Advancing Technology has Created a Need for Change in the "System of Records" Analysis' (2002-3) 39 *California West Law Review* 395, 399.
[196] Ibid.
[197] Ibid. See also 402-12 where Sullivan provides a detailed analysis of the system of records problem with respect to developing technology.
[198] *Doe v. Chao*, 540 U.S. 614, 617, 627 (2004) (Souter J.). This case involved a claim for workers' compensation. Doe's social security number appeared on multicaptioned hearing notices sent by the agency to a variety of third parties including lawyers and other claimants.
[199] *Whalen v. Roe*, 429 U.S. 589, 605 (1977) (Stevens J).

Act). [200] The amendments extended the *Wiretap Act's* coverage to encompass electronic communications. [201] Congress had initiated the changes in response to the decisions in *Katz* and *Berger*. [202]

Title 1 of the ECPA contains the *Wiretap Act* and Title II, the *Stored Communications Act*. ("*SCA*") [203] The *Wiretap Act* prohibits unauthorised interceptions of wire, oral and electronic communications, and the *SCA* prohibits unauthorised access to stored communications. [204] Although the ECPA is the overarching statute, discussion in the literature tends to focus on the individual components. I have followed this practice below.

Wiretap Act

The *Wiretap Act* prohibits the unlawful interception of wire, oral and electronic communications. An intercept is: [205]

> the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device

An electronic communication is: [206]

> any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio ,electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include –

---

[200] *Omnibus Crime Control and Safe Streets Act of 1968*, Pub. L. No. 90-351, 82 Stat. 197 (1968). See Michael D. Roundy, 'The Wiretap Act-Reconcilable Differences: A Framework for Determining the "Interception" of Electronic Communications Following United States v. Councilman's Rejection of the Storage/Transit Dichotomy' (2006) 28 *Western New England Law Review* 403, 411-16.

[201] *Steve Jackson Games Inc. v. United States Secret Service*, 36 F.3d 457, 460 (5th Cir. 1994) (Barksdale J).

[202] Ray Lewis, 'Employee E-mail Privacy Still Unemployed: What the United States Can Learn from the United Kingdom' (2007) 67 *Louisiana Law Review* 959, 965.

[203] 18 U.S.C. §§ 2510-2522 (*Wiretap Act*) 18 U.S.C. §§ 2701-2712 (*SCA)*. The ECPA also contains the *Pen Register Act* that regulates the use of pen registers and trap and trace devices. Pen registers record phone numbers (not the content of the communication) dialled by the target telephone. Trap and trace devices record the phone numbers of incoming calls: See Daniel J Solove, Marc Rotenberg, and Paul M. Schwartz, *Information Privacy Law* (2006), 271.

[204] §§ 2511, 2701(a).

[205] § 2510(4).

[206] § 2510(12).

> (A) any wire or oral communication;
> (B) any communication made through a tone-only paging device;
> (C) any communication from a tracking device (as defined in section 3117 of this title); or
> (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

Thus, an electronic communication would encompass email, the Internet, and video footage. However, the ECPA does not regulate the use of silent video recording. [207] This is because the Act "…technically applies only where oral communications are recorded along with the physical activity captured by the camera." [208] Although with respect to the use of cameras for law enforcement related purposes, federal law is inconclusive regarding the applicability of the Act "…to targeted silent video surveillance..." where an expectation of privacy exists in such circumstances. [209]

Unlawfully intercepting a communication may result in a fine or imprisonment for up to 5 years. [210] The Act also allows for civil action where there is an unlawful interception, disclosure, or use of a person's wire, oral or electronic communication. [211] Preliminary, equitable, or declarative relief, damages (including punitive damages), plus reasonable attorney's fees and litigation costs are recoverable. [212] Generally, this means actual damages plus any profits made by the offending party, [213] or statutory damages of $100 per day for each day of the violation or $10,000 whichever is greater. [214]

As with the Fourth Amendment, in order to seek protection under the ECPA, a person must demonstrate a subjective expectation of privacy that society would consider

---

[207] *Thompson v. Johnson County Community College*, 1997 U.S. App. LEXIS 5832, *3-4 (Porfilio J).
[208] Daniel D. Blinka 'Overview of Chapter 119. Wire and Electronic Communications Interception and Interception of Oral Communications' (2006) LEXSTAT *18 US NITA PREC 2510*, 1.
[209] Robert D. Bickel, Susan Brinkley and Wendy White, 'Seeing Past Privacy. Will the Development and Application of CCTV and Other Video Security Technology Compromise an Essential Constitutional Right in a Democracy, or Will the Courts Strike a Proper Balance?'(2003) 33 *Stetson Law Review* 299, 315-6 (and cases cited therein).
[210] § 2511(4)(a).
[211] § 2520(a). Plaintiff can recover from any party except the United States.
[212] § 2520(b)(1)-(3).
[213] § 2520(c)(2)(A).
[214] § 2520(c)(2)(B).

reasonable. [215] What is reasonable is determined on a case-by-case basis. [216]

The *Wiretap Act* contains three statutory exceptions. Commonly known as the service provider, the consent, and the business extension exception, they offer complete defences to intrusions and thus affect the ability of plaintiffs to seek appropriate remedies.

Under the service provider exception it is lawful for officers, employees or agents of providers of wire or electronic communication services "…to intercept, disclose, or use…" communications "…in the normal course…" of their employment "…while engaged in any activity which is a necessary incident to the rendition…" of the "…service or to the protection of the rights or property of the provider…" of the communication service. [217] The section also prohibits those who provide wire communication services to the public from observing or conducting random monitoring activities in relation to that service "…except for mechanical or service quality control checks." [218]

Lewis notes, "…Congress's statutory construction and unclear language have made this exception vague and led to confusion within the law." [219] Congress did not distinguish public from private service providers, nor define what constitutes actions done in the "normal course of employment" or what is "necessarily incident" to providing the communication service. [220]

This may mean that where an employer is a service provider they can lawfully monitor their employees' communications for a variety of business reasons. [221] In addition, the prohibition on random monitoring does not apply to electronic communication systems

[215] *Benford v. American Broadcasting Companies, Inc.*, 554 F. Supp. 145,154 (D.Md 1982) (Northrop S.J.).
[216] Ibid.
[217] § 2511(2)(a)(i).
[218] § 2511(2)(a)(i).
[219] Lewis, above n 202, 971.
[220] Ibid.
[221] See Mary E Pivec and Susan Brinkerhoff, 'E-Mail in the Workplace: Limitations on Privacy' (1999) 26(1) *Human Rights* 22.

leaving email "…susceptible to random interception, and accordingly more vulnerable to privacy invasions than voice mail messages." [222]

Interceptions are also lawful where a person is party to the communication or one of the parties to the communication has given prior consent to the interception. [223] However, consent "…is not necessarily an all or nothing proposition; it can be limited." [224] For example, where an employee only consents to the monitoring of business related phone calls. [225] In such circumstances consent extends to "…the inadvertent interception of a personal call, but only for as long as necessary to determine the nature of the call." [226]

Consent may be implied where the surrounding circumstances indicate a person "…knowingly agreed to the surveillance." [227] Although the circumstances relevant to the determination of consent may vary, "…the compendium will ordinarily include language or acts which tend to prove (or disprove) that a party knows of, or assents to, encroachments on the routine expectation that conversations are private." [228]
An employee may impliedly consent to monitoring where they have knowledge of its existence. [229] However, the Act "…expresses a strong purpose to protect individual privacy by strictly limiting the occasions…" where lawful interceptions occur, thus consent "…is not to be cavalierly implied." [230]

There is also protection from liability where an interception occurs by the operation of "…any telephone or telegraph instrument, equipment or facility, or any component thereof…" used in the ordinary course of the company's business. [231] Lewis describes this as the "…most unnerving exception to ECPA liability…" having the effect of

[222] Thomas R. Greenberg, 'E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute' (1994) 44 *American University Law Review* 219, 237 (and references therein).
[223] § 2511(2)(c),(d).
[224] *Watkins v. L.M. Berry & Co*, 704 F.2d 577, 582 (11th Cir. 1983) (Smith J) – refering to § 2511(2)(d).
[225] Ibid 581.
[226] Ibid.
[227] *United States v. Amen*, 831 F.2d 373, 378 (2nd Cir. 1987) (Oakes J).
[228] *Griggs-Ryan v. Smith*, 904 F.2d 112, 117 (1st Cir. 1990) (Selya J).
[229] See *Lukas v. Triborough Bridge and Tunnel Authority*, 1993 U.S. Dist. LEXIS 21065, *26-7 (Sifton J).
[230] *Watkins v. L.M. Berry & Co*, 704 F.2d 577, 581 (11th Cir. 1983) (Smith J).
[231] § 2510(5)(a)(i). Or used by a service provider in the ordinary course of business, or investigative or law enforcement officers in the ordinary course of their duties: § 2510(5)(a)(ii).

insulating "… employers from liability if they use certain devices to monitor their employees." [232]

Because the exception encompasses devices "…furnished to the subscriber or user by a provider…" of communications services, it permits employers who outsource such services to a third party to avoid liability where the interception of the communication occurs as part of normal business activities. [233] Although the Act does not define "ordinary course of business" this "… generally requires that the use be (1) for a legitimate business purpose, (2) routine and (3) with notice." [234]

When determining whether a breach has occurred the courts can consider the circumstances surrounding the interception including whether notice exists, and whether the interception was for a legitimate business purpose ("context approach").[235] Alternatively, courts focus on content of the communication, asking whether it was for business or personal reasons ("content approach"). [236]

Stored Communications Act

The *Wiretap Act* only prevents the interception of communications while in transit, thus does not provide protection for communications that are stored in databases, servers or similar. The *Stored Communications Act* (*"SCA")* prohibits intentional unauthorised access to communications in electronic storage. [237] Electronic storage includes temporary and intermediate storage of wire or electronic communications, such storage being incidental to its transmission, and storage of communications as part of a backup procedure. [238] The *SCA* also makes it unlawful for public service providers to disclose

[232] Lewis, above n 202, 972.
[233] § 2510(5)(a)(i); Rachel Sweeney Green, 'Privacy in the Government Workplace: Employees' Fourth Amendment and Statutory Rights to Privacy' (2004-5) 35(3) *Cumberland Law Review* 639, 649-50.
[234] *Adams v. City of Battle Creek*, 250 F.3d 980, 984 (6th Cir. 2001) (Merritt J).
[235] Lewis, above n 202, 972 (and references therein).
[236] Ibid.
[237] § 2701(a)(1),(2).
[238] § 2510(17).

the contents of an electronic communication while it is in electronic storage. [239]

Where an offence is committed under the *SCA* for "…commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State…" the maximum penalty is a fine and/or five years imprisonment for a first offence. [240] In addition, the aggrieved party may take civil action. [241] Appropriate preliminary and other equitable or declaratory relief, damages, legal fees, and other litigation costs reasonably incurred are recoverable. [242] As with the *Wiretap Act* actual damages suffered are recoverable plus any profits made by the offending party because of the unauthorised access (minimum of $1000). [243]

The *SCA* contains two relevant exceptions. The service provider exception removes liability "…with respect to conduct authorized – (1) by the person or entity providing a wire or electronic communications service;…." [244] This means that if an employer is a service provider, they may lawfully be able to access an employee's stored communications.

For instance, in *Bohach v. The City of Reno*, the Court found that when the Reno Police Department accessed stored messages of two of its employees, this was not a breach of the Act because the Department was a service provider. [245] Similarly, in *Fraser,* the Court found an insurance company's search of a former agent's emails fell within the scope of the exception because the company administered the network on which the

---

[239] § 2702(a)(1).
[240] § 2701(b)(1)(A). Subsequent offences attract a fine and/or imprisonment for not less than 10 years: § 2701(b)(1)(B). In other cases, punishment is a fine and/or imprisonment for not more than one year for a first offence or fine and/or imprisonment for five years for subsequent offences: § 2701(2).
[241] § 2707(a).
[242] § 2707(b)(1)-(3).
[243] § 2707(c). Punitive damages are also available where the violation is willful or intentional. Successful litigants under this section may also receive litigation costs and reasonable attorney's fees.
[244] § 2701(c)(1). Unlike the *Wiretap Act* the exception applies regardless of purpose: see Katherine A. Oyama 'E-Mail Privacy after United States v. Councilman: Legislative Options for Amending ECPA' (2006) 21 *Berkeley Technology Law Journal* 499, 507.
[245] *Bohach v. The City of Reno*, 932 F. Supp. 1232, 1236 (D.Nev. 1996) (Reed J).

emails were stored. [246] A provider of communications services to the public can also disclose the contents of a communication where one of the parties to the communication consents. [247]

The Intersection of the Wiretap and Stored Communications Acts

An issue courts face when assessing violations of the ECPA is determining whether the action in question constitutes an interception under *the Wiretap Act*, or whether it is unauthorised access to a stored communication in violation of the *SCA*. [248] This distinction can be important with respect to workplace intrusions, as employers charged under the *SCA*, are in a better legal position because the prohibition against interception is more stringent. [249] The following case law illustrates some of the difficulties faced by courts when addressing this issue.

Fraser v. Nationwide Mutual Insurance Co involved a dispute over the defendant company's termination of an agency agreement. [250] Before terminating his agreement, and acting on concerns that Fraser's emails might demonstrate improper behaviour on his part, the company searched its file server and located emails substantiating their concerns. [251] Fraser filed suit relevantly claiming the company had intercepted his email, and gained unauthorised access to his email while in storage in violation of the ECPA (and the Pennsylvanian state counterpart). [252]

Judge Ambro writing for the Court noted that "[e]very circuit court to have considered the matter has held that an 'intercept' under the ECPA must occur contemporaneously

[246] *Fraser v. Nationwide Mutual Insurance Co Inc.*, 352 F.3d 107, 115 (3rd Cir. 2003) (Ambro J).
[247] § 2702(b)(3).
[248] This involves the question of whether an interception has to occur contemporaneously with the transmission of the communication. This is a particular problem with respect to email systems as they perform both transmission and storage functions: see Charles H. Kennedy, 'U.S. Court Affirms Employer's Right to Read Employees' Email' (2005) *LexisNexis Martindale-Hubbell Legal Articles*.
[249] Ibid.
[250] *Fraser v Nationwide Mutual Insurance Co Inc.*, 352 F.3d 107, 109 (3rd Cir. 2003) (Ambro J). The parties disagreed over the reasons for termination.
[251] Ibid 110.
[252] Ibid 113-15.

with transmission." [253] In finding the company's actions did not constitute an interception, the Court held that although the definition of "intercept" adopted by Congress "…does not appear to fit with its intent to extend protection to electronic communications, it is for Congress to cover the bases untouched." [254]

In *Konop v. Hawaiian Airlines* the plaintiff operated a private secure website where he posted material critical of his employer (including its officers) and the pilot's union. [255] The vice-president of the company, concerned that Konop had posted untruthful allegations, used another employee's username and password (with that employee's consent) to access the site. [256] Konop filed suit against the airline relevantly claiming the vice-president's actions constituted either an interception, or alternatively, unlawful access to a stored communication. [257]

Judge Boochever noted that the intersection of the *Wiretap Act* and the *SCA* " '…is a complex, often convoluted, area of the law…' " and adding to the difficulty in the present case is "… the fact that the ECPA was written prior to the advent of the Internet and the World Wide Web." [258] The Court held that in order to violate the *Wiretap Act* the vice-president would need to have intercepted Konop's website "…during transmission, not while it is in electronic storage." [259] Thus, the vice-president's actions did not constitute a violation of the *Wiretap Act.* [260] However, instead of accessing the site by username and password, had the vice-president used monitoring software to capture the screen of Konop's computer while Konop was using the website, this would have violated the ECPA. [261] However, the Court concluded that because the vice-president was not a registered user, and the user details he used belonged to an employee who had never visited the site (thus was not authorised conduct by a "user" of the site in

[253] Ibid 113.
[254] Ibid 114.
[255] *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 872 (9th Cir. 2002) (Boochever J).
[256] Ibid 873.
[257] Ibid.
[258] Ibid 874 (Citing in part *United States v. Smith*).
[259] Ibid 878.
[260] Ibid 879.
[261] H. Joseph Wen , Pamela Gershuny, 'Computer-based monitoring in the American workplace: Surveillance technologies and legal challenges' (2005) 24 *Human Systems Management* 165, 171.

terms of § 2701(c)(2)), that the vice-president's actions constituted unauthorised access under the *SCA.* [262]

The most recent major Court of Appeal case to discuss the matter has not managed to clarify the issue. In the *United States v. Councilman,* the Defendant/appellee (Councilman) ran a company (Interloc), which provided an online out of print book listing service to book dealers. [263] Councilman directed his employees to intercept and copy emails sent by Amazon.com to book dealers. [264] In furtherance of this, Interloc's systems administrator made some modifications to the server's mail delivery software (procmail). [265] The changes meant before delivering email messages sent by Amazon.com to the dealers, procmail would forward a copy to a mailbox accessible by Councilman. [266] Councilman and his employees routinely read Amazon's emails in the hope of gaining some commercial advantage. [267]

Councilman argued the emails processed by procmail were not electronic communications, and the method used by the program to copy the emails did not constitute an interception under the *Wiretap Act.* [268] Judge Lipez for the en banc majority rejected "…Councilman's proposed distinction between 'in-transit' and 'in-storage' " [269] holding that an electronic communication encompasses "…transient electronic storage that is intrinsic to the communication process for such communications." [270] Further, "…an e-mail message does not cease to be an 'electronic communication' during the momentary intervals, intrinsic to the communication process, at which the message

---

[262] *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 880 (9th Cir. 2002) (Boochever J). It is possible for the acquisition of information on a website to constitute an intercept. Where identifying personal information was found on the servers of a company that provided pharmaceutical companies with software to monitor visits to their websites, the Court found that such acquisition occurred contemporaneously with the transmission of information by the users to the pharmaceutical companies: *In Re Pharmatrak, Inc. Privacy Litigation,* 329 F.3d 9, 12, 22 (1st Cir. 2003) (Lynch J).

[263] *United States v Councilman,* 418 F.3d 67, 70 (1st Cir. 2005) (Lipez J.). Interloc also provided the book dealers with an email address.

[264] Ibid 70.

[265] Ibid.

[266] Ibid.

[267] Ibid 70-1.

[268] Ibid 72. Councilman argued that when acquired the emails "…were in transient electronic storage…" and thus could not be subject to interception under § 2511(1)(a) (79).

[269] Ibid 79.

[270] Ibid.

resides in transient electronic storage." [271]

The Councilman Court may have decided not to add to this debate "…perhaps because it saw no analytically acceptable way to do so given the obtuse, technologically outdated language of the ECPA." [272] There also remain other unresolved issues, including that the definition of intercept "…is confusing and such ambiguity is likely to lead to conflicting interpretations in federal court." [273] There is also the immunity provided to ISP's with respect to the reading customers emails unless such actions constitute an interception, and the "…unequal protection for the contents of an e-mail based on technical evaluations of the physical point at which it was obtained rather than the underlying privacy interest." [274]

In response to the decision in *Councilman* a Bill was introduced into Congress to amend the definition of intercept. [275] The revised § 2510(4) read as follows: [276]

> "intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication ~~through the use of any electronic, mechanical, or other device~~ contemporaneous with transit, or on an ongoing basis during transit, through the use of any electronic, mechanical, or other device or process, notwithstanding that the communication may simultaneously be in electronic storage;

The change sought to clarify that an intercept under the *Wiretap Act* would "…include searches that are functionally real-time, in-transit acquisitions, regardless of whether they occur in temporary storage." [277] The Bill remains in committee.

Along with email and the use of video cameras, the Internet also poses problems for the ECPA. The Internet transmits a variety of communications including web pages, computer commands, music files, and others creating "… a communications network

---

[271] Ibid.
[272] President and Fellows of Harvard College, 'A Thinly Veiled Request for Congressional Action on E-Mail Privacy: United States v. Councilman' (2005) 19 *Harvard Journal of Law and Technology* 211, 227.
[273] Oyama, above n 244, 517.
[274] Ibid.
[275] H.R. 3503, E-Mail Privacy Act of 2005, 109th Cong., 1st Sess. (2005).
[276] § 2.
[277] 'Inslee Introduces Bipartisan Bill to Restore E-Mail Privacy' (29 July 2005) <http://www.house.gov/inslee/issues/privacy/tech_email_privacy.html> at 12 December 2007.

that supports a range of hardware and software that together foster a virtual world of cyberspace." [278] This "…multifunctionality creates a series of puzzling problems that complicates attempts to apply the Wiretap Act to it." [279] For example "…who is a 'party to the communication' who can consent to monitoring in the case of a human-to-computer or computer-to-computer communication? " [280]

The exceptions also provide some concern. Once an exception is "…successfully asserted, the ECPA fails to place any restrictions on the form and extent of such exempted monitoring." [281] Thus, "…the overall effect of the exceptions is to completely offset the protections afforded under the ECPA." [282] Lewis concludes that "[t]he only certainty connected to the ECPA is that it fails across the board to protect the privacy rights an individual, especially an employee, may have in his e-mails." [283]

The ECPA however remains an important source of protection for government employees when the circumstances of the intrusion do not fall within the Fourth Amendment, or where a court determines the statute provides sufficient constitutional protection thus pre-empting recourse to the Fourth Amendment. [284] It also provides a source of redress to private sector employees who have no recourse to protection under the Fourth Amendment.

Proposed Workplace Privacy Legislation

There have been three notable attempts to enact specific workplace privacy legislation at the federal level. The proposed measures offer varying degrees of protection, with some allowing employees to pursue personal remedies. The Bills are significant for a number of reasons.

---

[278] Orin S. Kerr, 'Internet Surveillance Law after the USA Patriot Act: The Big Brother that Isn't' (2003) 97 *Northwestern University Law Review* 607, 662 (Citing Gralla, Lessig).
[279] Ibid.
[280] Ibid.
[281] Lewis, above n 202, 973 (Citing Kesan).
[282] Ibid.
[283] Ibid.
[284] See *Adams v. City of Battle Creek*, 250 F.3d 980, 986 (6th Cir. 2001) (Merritt J); *Walker v. Darby*, 911 F.2d 1573, 1578-9 (11th Cir. 1990) (Peckham J); Green, above n 233, 648.

Firstly, if enacted they would provide a national framework offering a complaint process to employees regardless of sector or industry, many of whom currently have little or no redress against intrusions caused by electronic monitoring. The Bills also contain some constructive provisions that can assist in the development of uniform legislation in Australia. Importantly, the *Privacy for Consumers and Workers Act* in particular, offers more comprehensive protection to employees than is currently available through existing federal or state measures.

(a) Privacy for Consumers and Workers Act

In 1990 and again in 1993 Senator Paul Simon introduced the *Privacy for Consumers and Workers Act* ("PCWA") into the United States Senate. [285] The proposed Act requires the Secretary of Labor provide written notice to employees informing that their employer conducts or may conduct monitoring, and specify the circumstances where additional notice is or is not required. [286] The notice must also outline an employee's rights and protections under the Act. [287] Where an employer engages in electronic monitoring they must post this notice "…in conspicuous places on its premises where notices to employees are customarily posted." [288]

Additionally, employers are required to provide each employee (or their authorised representative) with prior written notice of electronic monitoring activities that will affect them. [289] The notice must include the following details: [290]

> (1) The forms of electronic monitoring to be used.
> (2) The personal data to be collected.
> (3) The hours and days per calendar week that electronic monitoring will occur.
> (4) The use to be made of personal data collected.
> (5) Interpretation of printouts of statistics or other records of information collected through electronic monitoring if the interpretation or records may affect one or more of the employer's employees.

[285] S. 984, Privacy for Consumers and Workers Act, 103d Cong., 1st Sess. (1993). Rep. Pat Williams introduced complimentary legislation into the House.
[286] § 4(a)(1)(A).
[287] § 4(a)(1)(B).
[288] § 4(a)(2).
[289] § 4(b).
[290] § 4(b)(1)-(9).

(6) Existing production standards and work performance expectations.
(7) Methods for determining production standards and work performance expectations based on electronic monitoring statistics if the methods affect the employees.
(8) A description of the electronic monitoring.
(9) A description of the exception that is authorized under section 5(c)(1) to be undertaken without notice.

Upon request, or at the time of offering employment, an employer is also required to provide prospective employees with such notice; [291] otherwise, notification of monitoring that may affect them must occur at their first interview. [292] Should members of the public (who are not customers of the employer) be subject to electronic monitoring, the employer must provide notice in a "…form that is reasonably calculated to reach members of the public who may be affected." [293]

There is an exception to the notice requirement where an employer reasonably suspects an employee is, or is about to, engage in conduct which would violate "…criminal or civil law, or constitutes willful gross misconduct; …" having "…a significant adverse effect involving economic loss or injury to the employer or employer's employees." [294] In such circumstances, before engaging in monitoring, an employer must execute a written statement detailing the conduct and the reasons for engaging in monitoring, identify the particular loss or injury resulting from the conduct, and state compliance with this section. [295]

Apart from the notice requirements, the PCWA contains a number of other protections for employees. For instance, periodic or random monitoring of new employees is authorised where "…the cumulative total period of such employee's employment with the employer is not more than 60 working days." [296] Existing employees with at least 5 years cumulative service are exempt from periodic or random monitoring. [297]

[291] § 4(c)(2).
[292] § 4(c)(1).
[293] § 4(e).
[294] § 5(c)(1). This does not apply where the employer is a Federal or State government entity.
[295] § 5(c)(2)(A)-(C). An employer must retain this statement for 3 years from the date of monitoring or until judgment is rendered in any civil action brought by an employee, whichever is the later: § 5(c)(2).
[296] § 5(b)(1).
[297] § 5 (b)(3).

There are also limitations on an employer's ability to review monitoring data. With respect to continuous monitoring performed on a random or periodic basis, where the review occurs during monitoring such activity is restricted to data acquired using "…an electronic identifier, locator, or accessor,…." [298] A review conducted post monitoring must only involve "…specific data that the employer has reason to believe contains information relevant to an employee's work." [299]

The PCWA also imposes restrictions on the collection and disclosure of information acquired through monitoring. Generally, an employer can only intentionally collect an employee's personal information for work related purposes. [300] There is also a prohibition on monitoring in bathrooms, locker rooms, or dressing rooms, [301] and the use of hidden cameras. [302] In addition, an employer cannot monitor an employee exercising their First Amendment rights, except where monitoring is work related and the data collected was incidental to the employee's exercise of these rights. [303] Generally, employees must provide prior written consent before data is disclosed to a third party. [304] Employees can also request access to their personal record. [305] Employers cannot take any action against an employee based on data acquired through monitoring unless they

[298] § 6(a). An electronic identifier, locator, or accessor includes "…an electronic card or badge access system, telephone call accounting system…" or where "…the data is continuously monitored by an employer or appears simultaneously on multiple television screens or sequentially on a single screen."
[299] § 6(b).
[300] § 10(a). This does not apply where the employee was a customer at the time.
[301] § 10(b)(1)-(3).
[302] § 11(2). This does not apply to monitoring permitted without notice: § 5(c)(1), by law enforcement agencies: § 13(a), for investigations under workmen's compensation: § 13(b), or for monitoring conducted by intelligence agencies: § 13(c)(2). Cameras (and other electronic monitoring technologies) whose purpose is to acquire information in accordance with the Act may still collect incidental information that is not work related or which concerns an employee exercising their rights under the First Amendment: § 10(f).
[303] § 10(c)(1)(2). The First Amendment states "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."
[304] § 10(d)(1)-(4). Exceptions apply where the disclosure is to fellow employees for work purposes, to law enforcement officials pursuant to a warrant, to the public where the data contains evidence of illegal conduct by a public official, or where there is a significant impact on public health or safety, or to an exclusive bargaining agent.
[305] § 7(a). An employer is not required to provide access to review where under § 5(c)(1) a notice of monitoring has not been given: § 7(b)(1). However where the investigation is complete or disciplinary action has been instigated (whichever occurs first) then a review is permitted: § 7(b)(2).

have complied with the provisions of the Act. [306] The PCWA also prohibits employers from using data obtained through monitoring as the sole basis for evaluating work performance, or for setting production quotas or performance expectations. [307]

Employees are prohibited from waiving their rights under the Act in contract or otherwise. [308] The provisions also apply to third parties who conduct monitoring on behalf of an employer. [309]

Civil penalties of up to $10,000 per occurrence are possible for breaches of the Act by employers. [310] The Secretary of Labor can bring an action to restrain breaches, including seeking the issuance of restraining orders and injunctions. [311] An aggrieved employee (or prospective employee) may also file civil suit. [312]

The PCWA primarily regulates through the provision of notice, and has attracted some criticism due to the lack of regulation of the types of monitoring implemented, and that it "…does not consider the employee's reasonable expectation of privacy when determining if surveillance is acceptable." [313] It is also argued the PCWA creates privacy rights that are incompatible with other statutes which regulate electronic communications such as the *Wiretap Act.* [314] Other concerns include the legislation's lack of clarity, difficulties with interpretation and administration, and the potential burden on small business. [315]

---

[306] § 8(a).
[307] § 8(b).Except for employees who do not attend the workplace and deliver their work from the remote location electronically and such data is the only basis available for such purposes.
[308] § 12(d). Unless such is part of a written settlement.
[309] § 13(d).
[310] § 12(a)(1).
[311] § 12(b). This can also include "…employment, reinstatement, promotion, the payment of lost wages and benefits, and reasonable attorney fees and other litigation costs reasonably incurred."
[312] § 12(c).
[313] S. Elizabeth Wilborn, 'Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace' (1998) 32 *Georgia Law Review* 825, 851 (and references therein).
[314] Donald R. McCartney, 'Electronic Surveillance and the Resulting Loss of Privacy in the Workplace' (1994) 62 *University of Missouri-Kansas City Law Review* 859, 886. See also pages 882-91 for a detailed discussion of the Bill.
[315] Laurie Thomas Lee, 'Watch your E-Mail! Employee E-Mail Monitoring and Privacy Law in the Age of the "Electronic Sweatshop" ' (1994) 28 *John Marshall Law Review* 139, 168-9 (and references therein).

The PCWA however, is unique in United States privacy history in that it offers a comprehensive national framework for regulating electronic monitoring in the workplace. The Act would also have provided private and public sector employees with significant protections with respect to the collection and use of monitoring data. Importantly, it offers employees access to civil remedies. The potential benefits of the PCWA, led some commentators to invoke John Whittier's famous line - " 'For of all sad words of tongue or pen, The saddest are these: 'It might have been.' " [316]

(b) Notice of Electronic Monitoring Act

In contrast to the PCWA, the *Notice of Electronic Monitoring Act* (NEMA) is more limited in scope. [317] Administratively, the Bill sought to amend the ECPA by redesignating § 2711 as § 2712 and inserting a new § 2711 "Electronic monitoring in the workplace." [318] The focus of the Bill is on providing employees prior notice of electronic monitoring. [319] The notice must describe: [320]

> (1) the form of communication or computer usage that will be monitored;
> (2) the means by which such monitoring will be accomplished and the kinds of information that will be obtained through such monitoring, including whether communications or computer usage not related to the employer's business are likely to be monitored;
> (3) the frequency of such monitoring; and
> (4) how information obtained by such monitoring will be stored, used, or disclosed.

Unlike the PCWA there is no requirement the government provide notice. Notice given by the employer must be "…clear and conspicuous… " and provided to employees "…in a manner reasonably calculated to provide actual notice,…." [321] The Act contains an exception to the notice requirement where an employer reasonably believes an employee has violated the employer's or another's legal rights, and such conduct involves

[316] Vance Lockton and Richard S. Rosenberg, 'A Preliminary Exploration of Workplace Privacy Issues in Canada' (2006) Office of the Privacy Commissioner of Canada Contributions Program, 23.
[317] H.R. 4908, Notice of Electronic Monitoring Act, 106th Cong., 2d Sess. (2000) Rep. Canady of Florida and Rep. Barr of Georgia).
[318] § 2(a)(1).
[319] § 2711(a)(1).
[320] § 2711(b)(1)-(4).
[321] § 2711(b).

significant harm to the employer or others, and monitoring would produce evidence of such. [322] Frayer notes this "…exception requires the individualized suspicion that the Supreme Court refused to address in *O'Connor*." [323]

An aggrieved employee can take civil action and obtain actual damages, punitive damages, litigation costs reasonably incurred (including attorney's fees) plus other appropriate preliminary and equitable relief. [324] Damages awarded to an individual employee cannot exceed $20,000, and the aggregate amount of damages awarded against any one employer for a given violation is a maximum of $500,000. [325]

The only obligation on employers or protection for employees under NEMA is the provision of notice. [326] NEMA does not regulate any other aspects of monitoring and it is unclear exactly what constitutes actual notice. Although personal remedies are available, these do not relate to the nature or extent of any violation of an employee's privacy rights, but only apply where an employer fails to meet the notice requirements. There was opposition to NEMA from some employer groups who argued for instance that it might increase the potential for litigation. [327] Others however, saw the legislation as providing an important contribution to worker's privacy. [328]

(c) Employee Changing Room Privacy Act

In February 2005, Representatives Petri and Andrews introduced a Bill prohibiting video

[322] § 2711(c).
[323] Charles E. Frayer, 'Employee Privacy and Internet Monitoring: Balancing Workers' Rights and Dignity with Legitimate Management Interests' (2002) 57(2) *The Business Lawyer* 857, 870.
[324] § 2711(d).
[325] § 2711(d)(3).
[326] NEMA lacks any substantive information privacy rights and being "notice-only privacy law" does not limit employers conducting overt surveillance: see Nathan Watson 'The Private Workplace and the Proposed "Notice of Electronic Monitoring Act": Is "Notice" Enough?' (2001) 54 *Federal Communications Law Journal* 79, 95 (Citing the statement of Marc Rotenberg before the House Subcommittee on the Constitution).
[327] Ibid 97 (Citing Congressional Hearings - statement of Kenneth Segarnick). The reasons included that the Bill does not clearly stipulate the type of notice required, and requiring notice about the frequency of observations may mean employers have an increased duty of care.
[328] Jill Yung, 'Big Brother IS Watching: How Employee Monitoring in 2004 Brought Orwell's 1984 to Life and What the Law Should Do About It' (2005) 36 *Seton Hall Law Review* 163, 208 (Citing Congressional Hearings, statement of James X. Dempsey, Center for Democracy and Technology).

and audio monitoring in certain areas of the workplace. [329] The Bill prevents employers from monitoring employees when they are "… in a restroom facility, dressing room, or any other area in which it is reasonable to expect employees of the employer to change clothing." [330]

A civil penalty of up to $10,000 per violation applies (or up to $25,000 where an employer knowingly violates the Act). [331] In determining the penalty the Secretary of Labor shall consider: [332]

> (1) the nature, circumstances, extent, and gravity of the violation or violations; and
> (2) with respect to the violator, the ability to pay, effect on ability to continue to do business, any history of prior violations, the degree of culpability, and such other matters as justice may require.

The Secretary may also seek an injunction to prevent a violation of the Act. [333] An aggrieved employee may also file civil suit against their employer. [334] A court may grant an injunction prohibiting the current violation or preventing further violations, damages not exceeding $25,000 if the employer knowingly engaged in the activity, or both. [335] As with the Victorian legislation, the Act is limited to prohibiting only certain forms of monitoring in designated areas of the workplace. Similarly, there is also no requirement employees be provided with notice. Unlike Victoria however, employees can seek civil redress.

Other Measures

Other statutes at the federal level address various aspects of individual privacy. These include measures regulating the disclosure of an individual's health or educational information, the release of financial records, the use of polygraph testing in the

[329] H.R. 582, Employee Changing Room Privacy Act, 109th Cong., 1st Sess. (2005).
[330] § 2.
[331] § 3(a).
[332] § 3(c).
[333] § 3(h).
[334] § 4(a).
[335] § 4(a)(1)-(3).

workplace, the manner in which credit reporting agencies manage consumer data, and the disclosure of consumer information by video shop owners without the customer's consent. [336] For present purposes, the most relevant is the *Patriot Act*, enacted October 2001 in response to the terrorist attacks on September 11 of that year. [337]

Impact of the USA Patriot Act

The Act is not a new regulatory scheme as such, but operates by inserting amendments into existing statutes. [338] With respect to the ECPA, the *Patriot Act* amended the "…definition of 'wire communication' by moving the protection of stored voice communications - such as voice-mail messages – from the Wiretap Act to the SCA." [339] In combination with adding the term "wire" to § 2703, means the government now requires a search warrant rather than an interception order to access stored communications. [340] The requirements for an interception order are more stringent. [341]

Sproule argues "…employers may be tempted to 'cooperate' with the government and turn over records and stored communications without requiring the law-enforcement officials to obtain a warrant." [342] The Act also permits searches and seizures without having to immediately inform the subject of the search whether the purpose of the search is to locate evidence of a crime. [343] For example, where an employer is a service

[336] For details and discussion of these statutes see Laura Evans, 'Monitoring Technology in the American Workplace: Would Adopting English Privacy Standards Better Balance Employee Privacy and Productivity?' (2007) 95 *California Law Review* 1115, 1123; McCartney, above n 314, 876-8.

[337] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001*, Pub. L. No. 107-56 115 Stat. 272 (2001).

[338] Steven C Posner, 'Practice Commentary - Privacy and the USA Patriot Act' (2005) *LexisNexis Martindale-Hubbell Legal Articles*.

[339] Oyama, above n 244, 504.

[340] Clare M. Sproule, 'The Effect of the USA Patriot Act on Workplace Privacy' (2002) 43(5) *Cornell Hotel and Restaurant Administration Quarterly* 65, 72.

[341] A Federal judge hears applications for intercept orders: § 2518(1). In considering whether to grant such order the court requires quite extensive information including full details of the circumstances that justify the belief the order should be issued, whether other investigative procedures have been tried, and the length of time the interception is required: see § 2518(1)(a)-(f).

[342] Sproule, above n 340, 72.

[343] Nancy J. King, 'Electronic Monitoring to Promote National Security Impacts Workplace Privacy' (2003) 15(3) *Employee Responsibilities and Rights Journal* 127, 137. These are the delayed notification rules. Due to their covert nature, such searches are referred to as "sneak and peek" searches.

provider, a court order may require the employer access that employee's stored voice and email messages and supply them to the authorities without at that time providing any notification to the employee that this has occurred. [344]

Privacy Protection at the State Level

Constitutional

Some states have incorporated provisions similar to the Fourth Amendment in their constitutions, while others contain general privacy provisions. For example, the Californian Constitution describes privacy as an inalienable right. [345] Privacy protection under the Californian Constitution also extends to private organizations. [346]

The California Court of Appeal in a case involving the privacy of personal data stored on a company owned computer applied the Constitutional guarantee. [347] TBG requested Zieminski (a former employee) return a computer the company had provided to him so he could perform work at home. [348] TBG also asked him not to delete any information on the machine's hard drive. [349] Zieminski claimed he would have to delete some personal information before returning the computer. [350] TBG served a demand for production of the computer and Zieminski objected claiming an infringement of his Constitutional right to privacy. [351] The Court held that Zieminski did not enjoy a reasonable expectation of privacy with respect to the contents of the computer. [352] Before using the computer, Zieminski had signed TBG's computer use policy that explicitly stated the company owned the computer and that it was for company business

[344] Ibid. Once the delay period has expired, the government must inform the employee.
[345] Art. 1 § 1.
[346] *Hill v. National Collegiate Athletic Association*, 865 P.2d 633, 644 (1994) (Lucas CJ). The elements for an action for invasion of privacy under the Constitution are "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy." (657).
[347] *TBG Insurance Services Corporation v. Zieminski* (2002) 96 Cal. App. 4th 433 (Vogel J).
[348] Ibid 446.
[349] Ibid.
[350] Ibid 446-7.
[351] Ibid 447.
[352] Ibid 453 (and cases cited therein).

only. [353] The policy also stated that communications transmitted by company owned equipment were not private and that TBG personnel could at their discretion, monitor messages and files on company owned computers. [354] Referring to the establishment of such email and Internet use policies the Court held "…the use of computers in the employment context carries with it social norms that effectively diminish the employee's reasonable expectation of privacy…" with respect to the use of employer owned computers. [355]

There are also many state based equivalents to the ECPA. The focus here however is on specific workplace privacy legislation, and common law tort of invasion of privacy.

Workplace Privacy Legislation

A number of states including Delaware, Connecticut, California, West Virginia, and Rhode Island have enacted workplace privacy legislation. [356] For example in Delaware monitoring telephone conversations, email messages, or Internet access is prohibited unless the employer first provides notice at least once during the day when an employee access the facilities, or alternatively has given a "1-time" written notice detailing the company policy on monitoring. [357] Penalties under the Act are limited to $100 for each such violation. [358]

Some states have also attempted to enact workplace privacy measures. For instance, Georgia introduced a Bill containing provisions similar to the Federal Privacy for Consumers and Workers Act. [359] In 2004, the Californian Senate passed a Bill that

[353] Ibid 452.
[354] Ibid 453.
[355] Ibid 452. CF *Quon v. Arch Wireless Operating Company Inc.*, 2008 U.S. App. LEXIS 12766, *47 (Wardlaw J) where the 9th circuit found that a police officer's Californian constitutional (and Fourth Amendment) privacy rights were violated when *Arch Wireless* (the city's service provider) supplied the city police department transcripts of his text messages so they could conduct an audit to determine whether the messages were work related.
[356] *Delaware Labor Code,* Title 19, § 705 (2007); *Conn. Gen. Stat.* § 31-48d (2007); *Cal Lab Code* § 435 (2007); *R.I. Gen. Laws* § 28-6.12-1 (2007); *W. Va. Code* § 21-3-20 (2007). These and the proposed measures are discussed more fully in Chapter Three.
[357] *Delaware Labor Code,* Title 19, § 705(b).
[358] *Delaware Labor Code,* Title 19, § 705(c).
[359] Ga.H.B. 566, Privacy for Consumers and Workers Act, 144th Legis., 1st Sess. (1997-8).

prohibited electronic monitoring without notice. [360] Governor Schwarzenegger exercised his right of veto because amongst other things, he believed compliance with the provisions would unduly burden employers. [361]

Generally, the position in respect to the states is somewhat analogous to what has occurred at the federal level. However, in addition to constitutional and statutory protections, the other main avenue of redress, particularly for private sector employees, is the tort of invasion of privacy.

Tort Privacy

Unlike Fourth Amendment privacy which focuses on preserving secrecy with respect to government intrusions, tort privacy is concerned with "…controlling the flow of information about oneself in order to preserve individuality…." [362] To Warren and Brandeis, the common law was to be the basis for the recognition of what Judge Cooley termed "…the right 'to be let alone.' " [363] Remedies for breach were similar to that for defamation, that is, a tort action for damages and in limited cases injunctive relief. [364] Warren and Brandeis also thought it was "…desirable that the privacy of the individual should receive the added protection of the criminal law, but for this, legislation would be required." [365] It appears though it was Warren rather than Brandeis who favoured such a move. [366]

The *Restatement of Torts* first recognised the right to privacy in 1939, and by 1952, most

[360] Cal. Senate Bill 1841 (2003-4).
[361] Governor of California, 'Veto Note to the Members of the California State Senate' (29 September 2004) <http://www.leginfo.ca.gov/pub/03-04/bill/sen/sb_1801-1850/sb_1841_vt_20040929.html> at 5 February 2009.
[362] Gormley, above n 88, 1374.
[363] Samuel D. Warren and Louis D. Brandeis, above n 84, 195.
[364] Ibid 219.
[365] Ibid. William H. Dunbar, Esq. (of the Boston Bar) prepared a draft Bill (reproduced in fn 3 on page 219).
[366] Barron, above n 85, 912-3.

jurisdictions in the United States acknowledged its existence. [367] The *Second Restatement* outlines the general principle that a person who invades the privacy of another is subject to liability for the resulting harm. [368] Section 652A(2) contains the four torts identified by Prosser, that is, unreasonable intrusion upon the seclusion of another, appropriation of the other's name or likeness, unreasonable publicity given to the other's private life, and publicity that unreasonably places the other in a false light before the public. [369] The "unreasonable publicity" tort (§ 652D) appears to be what Warren and Brandeis envisaged in their article. [370]

The most relevant to workplace privacy is Intrusion Upon Seclusion ("Intrusion"). The *Restatement* defines Intrusion as: "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." [371]

The tort does not depend on any publicity given to the subject of the intrusion. [372] The intrusion can be by physical, electronic or other means. [373] Thus in accordance with the *Restatement* definition there must be:

1) an intentional intrusion;
2) into the private affairs of another;
3) in a manner which is highly offensive to a reasonable person.

Case law illustrates the difficulties plaintiffs have in establishing they enjoy a reasonable expectation of privacy in the workplace. In *Smyth v Pillsbury*, the company implemented

[367] James W. Hilliard, 'A Familiar Tort That May Not Exist in Illinois: The Unreasonable Intrusion On Another's Seclusion' (1999) 30 *Loyola University Chicago Law Journal* 601, 604 (and references therein).
[368] *Restatement (Second) of Torts* (1977), § 652A(1).
[369] Ibid § 652B-E. There are some differences in the wording of the actions: see William L. Prosser, 'Privacy' (1960) 48(3) *California Law Review* 383, 389.
[370] Barron, above n 85, 879 (and references therein).
[371] *Restatement (Second) of Torts* (1977), § 652B.
[372] Ibid com. a.
[373] Ibid com. b.

an internal email system to promote the exchange of corporate communications amongst its employees. [374] The company assured employees that their email communications would remain confidential, and could not be subject to interception and used as grounds for reprimand or termination. [375] In violation of these assurances, the company intercepted and examined Smyth's private email messages. [376] The company subsequently terminated Smyth's employment claiming he transmitted emails containing "…inappropriate and unprofessional comments…" over the company's network. [377] Smyth claimed the company's actions violated " '…public policy which precludes an employer from terminating an employee in violation of the employee's right to privacy as embodied in Pennsylvania common law.' " [378]

Judge Weiner contrasted the interception of Smyth's email with searches of personal property and urinalysis. [379] The Court held Smyth had no reasonable exception of privacy in emails he voluntarily sent over the company network, notwithstanding the assurances he received from the company. [380] Smyth had communicated the contents of the emails to a second person (his supervisor) over a network used by the entire company, thus forgoing any reasonable expectation of privacy he might have had in the information. [381] Unlike urinalysis or property searches, the company did not require Smyth to disclose personal information, he did so on his own accord. [382] Even if Smyth did have a reasonable expectation of privacy in the contents of his email, a reasonable person would not find the company's interception "… a substantial and highly offensive invasion of his privacy." [383]

The Court in *McLaren v Microsoft* reached a similar conclusion. [384] Microsoft suspended

[374] *Smyth v. Pillsbury Co*, 914 F. Supp. 97, 98 (E.D. Pa. 1996) (Weiner J).
[375] Ibid.
[376] Ibid.
[377] Ibid 98-99. The company alleged the emails contained threats against sales management staff and that Smyth also "…referred to the planned Holiday party as the 'Jim Jones Koolaid Affair.' " (fn 1).
[378] Ibid 100.
[379] Ibid 101.
[380] Ibid.
[381] Ibid.
[382] Ibid.
[383] Ibid.
[384] *McLaren v. Microsoft Corporation,* 1999 Tex. App. LEXIS 4103 (Roach J).

McLaren's employment pending an investigation over alleged improprieties. [385] McLaren requested access to his email to assist in refuting the allegations against him, however was told he must inform company officials where the emails were located and they would retrieve them for him. [386] Access to email was through a network login and password, however users could assign a separate password to their personal folders. [387] McLaren's personal folder was password protected. [388] McLaren told the company no one was to access his workstation or email. [389] Shortly afterwards Microsoft terminated McLaren's employment. [390]

McLaren sued for invasion of privacy claiming Microsoft had unlawfully accessed his personal folders on his office computer and distributed their contents to third parties. [391] Although it was possible for Microsoft to decrypt passwords and obtain access, McLaren argued that in allowing employees to place passwords on their personal folders Microsoft had acknowledged employees had a legitimate expectation that the folders were free from interference. [392]

McLaren attempted to draw an analogy between the storage of email in personal folders and items that are stored in an employee's locker. [393] The Court in *Trotti* however noted the locker in question was specifically for "…storing personal belongings, not work items." [394] Here Microsoft provided McLaren with a computer to perform his duties. [395] Further, "…the e-mail messages contained on the company computer were not McLaren's personal property, but were merely an inherent part of the office environment." [396] The locker referred to "…was a discrete, physical place where the employee, separate and apart from other employees, could store her tangible, personal

[385] Ibid *1.
[386] Ibid *1-2.
[387] Ibid *2.
[388] Ibid.
[389] Ibid.
[390] Ibid.
[391] Ibid.
[392] Ibid *2-3.
[393] Ibid * 9-10 (Citing *K-Mart Corp.Store No. 7441 v. Trotti*, 677 S.W.2d 632 (Tex. Ct. App. 1984).
[394] Ibid *11.
[395] Ibid.
[396] Ibid.

belongings." [397] In contrast, the email storage system "…is not so discrete." [398] Emails were initially stored on the server, however users could then move them to personal folders, and it was McLaren's usual practice to do so. [399] However, the email messages first passed over the network, making them at some point accessible to third parties. [400] Thus, even though McLaren created a personal password, this did not manifest a reasonable expectation of privacy on McLaren's behalf, nor did it require Microsoft to recognise such expectation, so the company was not precluded from assessing the folders. [401]

Even if McLaren did have a reasonable expectation of privacy in his emails, "…a reasonable person would not consider Microsoft's interception of these communications to be a highly offensive invasion." [402] Given McLaren "…had notified Microsoft that some of the e-mails were relevant to the investigation…the company's interest in preventing inappropriate and unprofessional comments, or even illegal activity, over its e-mail system would outweigh McLaren's claimed privacy interest in those communications." [403]

However, in *Fischer v. Mt. Olive Lutheran Church* (Connor) pastor at the defendant church engaged a computer expert who accessed the plaintiff's hotmail account and printed out his emails. [404] Connor also accessed the plaintiff's hotmail account on two further occasions. [405] Later the church dismissed the plaintiff (who was its Minister) over allegations of misconduct involving a telephone conversation and the content of some of

[397] Ibid.
[398] Ibid.
[399] Ibid *12.
[400] Ibid.
[401] Ibid.
[402] Ibid *13.
[403] Ibid. See also *Thygeson v. U.S. Bancorp*, 2004 U.S. Dist. LEXIS 18863, *60-72 (Stewart, Magistrate Judge). The Court found no expectation of privacy in emails in Thygeson's personal folder including emails transmitted via his personal email account; *Garrity v. John Hancock Mutual Life Insurance Company*, 2002 U.S. Dist. LEXIS 8343, *1-7 (Zobel J) where the Court reached a similar conclusion involving personal emails containing content in violation of the company's email policy even though these were stored in a password protected personal folder.
[404] 207 F. Supp. 2d 914, 920 (W.D. Wis. 2002) (Crabb J).
[405] Ibid 921.

the emails in his hotmail account. [406] The Court denied the defendant's motion for summary judgment with respect to the email on the basis "…it is disputed whether accessing plaintiff's email account is highly offensive to a reasonable person and whether plaintiff's email account is a place that a reasonable person would consider private,…." [407]

Corbett states that "[m]ost invasion of privacy claims in the employment context fail because courts find either that there is no reasonable expectation of privacy, or that the invasion would not be highly offensive to a reasonable person, or both." [408] Even where an employee has a reasonable expectation of privacy, they cannot pursue a cause of action unless they are "…viewed engaging in some sort of private activity, and activities that are work-related are generally not considered private vis-a-vis one's employer." [409] "For this reason, most employer surveillance of activities in the workplace will not be tortious." [410]

Another limitation is that employees may not have access to the appropriate information or have the financial means to pursue a civil suit. [411] In addition, even where an employee is successful, subsequent interpretation by the courts may see the judgment reversed. [412] Although a common law action is available to employees in both the public and private sectors, such would appear not to offer substantive protection against the potential threat to privacy rights posed by electronic monitoring in the workplace.

---

[406] Ibid 917-21.

[407] Ibid 928. *Federal Civil Procedure Rule 56* authorises summary judgment where there is no genuine issue of material fact and the moving party is entitled to judgment as a matter of law: see commentary in Prof. David A. Sonenshein, 'Rule 56. Summary Judgment' (2008) LEXSTAT *US NITA FED RULES CIV PROC R 56.*

[408] William R., Corbett, 'The Need For a Revitalized Common Law of the Workplace' (2003) 69 *Brooklyn Law Review* 91, 110 (and references therein).

[409] Daniel P. O'Gorman, 'Looking out for Your Employees: Employers' Surreptitious Physical Surveillance of Employees and the Tort of Invasion of Privacy' (2006) 85 *Nebraska Law Review* 212, 237.

[410] Ibid.

[411] Dennis P. Duffy, 'Intentional Infliction of Emotional Distress and Employment at Will: The Case Against "Tortification" of Labor and Employment Law' (1994) 74 *Boston University Law Review* 387, 423.

[412] Ibid 426 (and references therein).

Conclusion

Technology continues to provide challenges to employees' privacy rights. Both Australia and the United States have implemented a national framework for regulating personal information collected by government, and each has some form of statutory protection against electronic monitoring. Although the United States has a more diverse privacy enforcement regime, these measures for the most part do not offer sufficient protection to employees. Efforts in the United States to implement national regulation have been unsuccessful, although some state governments have introduced some limited statutory protection for employees.

Both New South Wales and Victoria have enacted workplace privacy legislation, although with respect Victoria, this is limited to prohibiting certain forms of monitoring in particular areas of the workplace. The *Privacy Act* and state based equivalents are not suitable for addressing many of the concerns that arise through the implementation of electronic monitoring. At this point it is uncertain how the tort of invasion of privacy will develop in Australia and how such will affect employees' chances of seeking effective redress.

The development of workplace privacy legislation in both nations is encouraging. However, the advent of new and improved technologies to conduct electronic monitoring, viewed against the backdrop of current regulatory measures, suggests that existing measures are inadequate to address concerns over the potential threat to employees' privacy rights posed by electronic surveillance. With this in mind, Chapter Three further examines the ability of current measures to protect an employee's privacy against intrusions caused through the continued use of monitoring in the workplace.

Chapter Three

An Examination of the Complaint Process and Remedies Available to Employees for Intrusions Caused by Electronic Monitoring

Introduction

This chapter provides a contextual survey of the complaint process and remedies available to employees in Australian and the United States. To illustrate the manner in which existing legal and other measures operate in practice, the following analysis eschews a purely descriptive account of cataloguing avenues of redress by adopting instead, a contextual approach based on a hypothetical employee (Mary) who is concerned about protecting her privacy rights at work. There is also an examination of proposed statutory measures from both jurisdictions.

Using a case model to illustrate the relevant issues inevitably leads to some overlap with the material outlined in the previous chapter. However, the focus here is to provide practical advice to a fictitious employee concerned about her privacy in the workplace. Adopting this approach allows for the examination of the issues in greater depth and assists in the development of the draft legislation detailed in Chapter Five.

Mary's Work Environment

Mary has worked for her current employer for over 10 years. She works in an open plan office performing administrative duties. Mary's employer has installed CCTV cameras throughout the workplace, including in the lunchroom, car park, and entrance foyer. Although the cameras have audio capabilities, this function is not used.

Mary's employer provides her with a computer and access to email and the Internet through the company's network. Mary mostly uses email and the Internet to perform work related tasks, though on some occasions, she sends private emails and accesses non-work related websites.

On Mary's first day of work, her employer provided her with a copy of the computer usage policy. The policy also appears on the company's website. The policy does not prohibit employees from using employer-supplied facilities for personal reasons, but states such use should be limited, and that employee communications may be subject to monitoring.

Mary is concerned that some of her personal information may be collected through monitoring. She is also worried about who may have access to this information. There is also the issue of whether her employer may use the data for performance evaluation or as evidence in disciplinary proceedings. Mary is also troubled about the overall extent of video monitoring, particularly whether her employer is using hidden cameras.

Process and Remedies for Privacy Intrusions in the Workplace

The following discussion focuses on the complaint process and remedies available to Mary under workplace privacy legislation in Australia and the United States. With respect to Australia, only New South Wales and Victoria have enacted such measures. Therefore, I also examine Mary's options under information privacy laws (or administrative instruments where applicable). Lastly, I consider the possibility of Mary instigating an action at common law.

At the federal level in the United States, I examine Mary's options with respect to the *Privacy Act*, the *Electronic Communications Privacy Act*, the Fourth Amendment, and several proposed national workplace privacy initiatives. I also canvass several existing and proposed state based statutory measures, and the tort of Intrusion Upon Seclusion.

AUSTRALIA

Commonwealth /Australian Capital Territory

There is no specific workplace privacy legislation at the national level. The *Privacy Act*

1988 applies to records held by Commonwealth and Australian Capital Territory government departments, and to information collected by private sector organizations covered by the Act. A consideration of Mary's options under this legislation follows below.

The Privacy Act

Regardless of the nature and extent of monitoring conducted by Mary's employer, recourse to the Act is only possible where there is a breach of the Information Privacy Principles ("IPP's"). This would include for example, where Mary's employer collects personal information for an unauthorised purpose, or fails to securely store the information, or discloses her personal data to third parties without first obtaining her consent. [1] General concerns regarding the number and type of devices used, their location or similar issues, would usually not constitute sufficient grounds for complaint.

The Act treats public and private sector employees somewhat differently. If Mary is in the public sector and believes her employer's monitoring has breached the IPP's, she can lodge a written complaint with the Privacy Commissioner. [2] The Commissioner's role includes the investigation of potential breaches by agencies of the IPP's and if appropriate, attempt settlement through conciliation. [3]

There are a number of reasons why the Commissioner may decline to investigate Mary's complaint. These include where no breach has occurred, where Mary complains more than 12 months after she became aware of the alleged breach, or where the complaint is frivolous, vexatious or otherwise lacking substance. [4] The Commissioner may also decline to investigate the complaint where Mary has not first sought to resolve the issue directly with the responsible agency. [5] According to the 2006-7 Annual Report the

1 s 14 (Principles 1, 4, 11).
2 ss 36(1), 36(3).
3 s 27(1)(a).
4 See s 41(1)(a)-(f).
5 s 40(1A). Unless the Commissioner decides this is not appropriate in the circumstances.

Commissioner declined to investigate 52% of written complaints received. [6]

The Commissioner may conduct preliminary enquires with the respondent agency to determine whether he or she has the power to investigate the complaint, or whether discretion exists with respect to declining to investigate the matter. [7] During the 2006-7 financial year, the Commissioner closed 36% of all complaints after making such inquiry. [8]

The Commissioner may formally investigate Mary's complaint. [9] The Commissioner has wide powers to obtain information and documents, examine witnesses and direct persons to attend compulsory conferences. [10] Of the total complaints received during the 2006-7 financial year only 12% were subject to formal investigation. [11]

Once the investigation is completed, the Commissioner may decide to dismiss Mary's complaint, [12] or uphold the complaint and make a determination. [13] This may include awarding Mary monetary compensation. [14] There were no determinations made during 2006-7. [15]

As determinations are neither binding nor conclusive between the parties to the complaint, [16] Mary may need to commence proceedings in the Federal Court or Federal Magistrates Court to enforce the determination. [17] The proceedings are by way of a de novo hearing. [18] Mary can also apply for legal assistance. [19] The court may make any

---

6 Office of the Privacy Commissioner, 'The Operation of the Privacy Act Annual Report 1 July 2006-30 June 2007' (2007), 49.
7 s 42.
8 Office of the Privacy Commissioner, above n 6, 49.
9 s 40(1).
10 ss 44-6.
11 Office of the Privacy Commissioner, above n 6, 49.
12 s 52(1)(a).
13 s 52(1)(b).
14 s 52(1)(b)(iii).
15 Office of the Privacy Commissioner, above n 6, 50.
16 s 52(1B).
17 s 55A(1)(a). The Commissioner can also take action to enforce a determination: s 55A(1)(b).
18 s 55A(5).
19 s 63(2).

order it thinks fits in the circumstances, including the granting of an injunction where appropriate. [20]

Alternatively, the parties may reach settlement through conciliation. This may also include awarding Mary compensation. During the 2006-7 financial year compensation was the most common resolution for investigated complaints, with the majority of payments being less than $2000. [21]

In *Seven Network (Operations) v MEAA* the television station wished to implement a new enterprise bargaining agreement with its employees. [22] A significant privacy issue arose when a call centre (engaged by the union) used details from a copy of Seven's internal telephone directory to poll employees about the proposed agreement. [23] The Court held that through commissioning the survey, instructing the call centre to acquire the information, and receiving a report, the union breached the Act, as these actions resulted in the collection of personal information unrelated to any of its functions. [24] The call centre was also in breach of Principle 1.3 as it had not disclosed its identity to the individuals it polled. [25] The Court further held, using section 80 of the *Trade Practices Act 1974* (Cth) as a guide, that the station was entitled to an injunction with respect to the union's breaches of the Act. [26] This is significant given that the station had not lodged a complaint with the Privacy Commissioner. [27] This decision means a complainant such as Mary could apply directly to the Federal Court for an injunction

---

[20] ss 55A(2), 98(1).

[21] Office of the Privacy Commissioner, above n 6, 51. Just over 30% of these complaints resulted in the payment of compensation. The amendment of records was the second most common outcome.

[22] *Seven Network (Operations) Limited v Media Entertainment and Arts Alliance* [2004] FCA 637, [3] (Gyles J).

[23] Ibid [5-23].

[24] Ibid [46], *Privacy Act* Schedule 3, Principle 1.1. There was also no compliance with Principle 1.5 (collecting information about an individual from a third party without taking reasonable steps to inform the individual concerned about the matters in Principle 1.3) and Principle 1.3 (requirements that include informing individuals about the purposes of the collection, and the consequences of not providing the information) – in relation to the script used by the call centre.

[25] Ibid [10],[11],[51]. The script instructed the operator to state that they were calling from the union.

[26] Ibid [55].

[27] Existing authority held that the Federal Court was limited to enforcing determinations made by the Privacy Commissioner: see Normann Witzleb, 'Federal Court strengthens privacy enforcement: Seven Network (Operations) Limited v Media Entertainment and Arts Alliance [2004] FCA 637' (2005) 33 *Australian Business Law Review* 45, 47 (Citing *Gao v Federal Privacy Commissioner*, *Ibarcena v Templar*).

without being required to go through the usual complaint process. [28]

Under the *Privacy Act* the Commissioner can enforce a determination against the responsible agency through the Federal Court. [29] The Commissioner where appropriate can also refer complaints to other relevant bodies such as the Ombudsman and the Public Service Commissioner. [30]

As an alternative, Mary can also seek to address her concerns through her Department's internal grievance process. One of the major grounds the Commissioner has given for declining to investigate matters further following an initial investigation is that the respondent agency has adequately dealt with the issue. [31]

In summary, as a public sector employee, Mary's remedies under the *Privacy Act* are dependent upon showing the monitoring of her email and Internet or the other activities such as video recording in lunchroom, or use of hidden cameras, or placement of cameras constitute a breach of the IPP's. Mary may also be able to complain about the use of the data for performance evaluation or similar, if when acquiring the information, her employer did not inform her that such was the purpose for collection.

Much would depend on the extent and scope of her employer's monitoring policy. However, it is unlikely general monitoring activities will breach the Act if they are in accordance with the IPP's. Some of the other activities, particularly with respect to the use of cameras, may potentially violate the Act. For example, this could be where the collection does not relate to a business function. Finally, even if the Commissioner investigates her complaint, only approximately 20% of the complaints with respect to the IPP's were upheld in 2006-7. [32]

---

[28] Ibid 49. Noting this decision was the first to invoke the injunctive power in the Act without the requirement to first lodge a formal complaint.
[29] s 62(1).
[30] s 50(2).
[31] s 41(2)(a), Office of the Privacy Commissioner, above n 6, 50. The Commissioner declined to investigate approximately 45% of complaints for this reason.
[32] Ibid 50.

In contrast, if Mary is in the private sector, her options are somewhat diminished. In particular, if Mary works for a small business, she has no recourse to the Act. [33] Even if Mary works for a larger organization, the employee records exemption would apply to any monitoring information forming part of her employment record. [34]

There is also uncertainty as to whether or not the private sector provisions of the Act protect personal email. [35] Even if they do, this may still pose problems, especially where employers conduct monitoring without appropriate guidelines. This is because "[t]he personal nature of email often makes it difficult to make a clear distinction between records relating to an employment relationship and other information disclosed through monitoring." [36]

Another issue is that if an employer's email policy treats incoming and outgoing email in the same way although they "…may rely on the employee record exemption to authorise monitoring, they may collect personal information about parties that are not employees." [37] Thus, there would need to be an examination of Mary's emails to determine whether any were clearly personal in nature before a determination concerning a breach of the privacy principles could occur.

Should Mary believe her employer's monitoring activities have breached the Act, and her company has an approved privacy code containing a process for resolving complaints, then Mary must first attempt to have her complaint determined by the

---

[33] ss 6C(1), 6D(1).

[34] s 7B(3). See Allens Arthur Robinson, 'Overview: Who, what and when: Exemptions' <http://www.aar.com.au/privacy/over/who/exemp.htm?print=true> at 23 March 2007. The *Privacy Amendment (Private Sector) Act 2000* (Cth) amended the Act with respect to private organizations. See generally Attorney-General's Department and Department of Employment and Workplace Relations, 'Employee Records Privacy - A discussion paper on information privacy and employee records' (February 2004); Margaret Otlowski, 'Employment Sector By-Passed by the Privacy Amendments' (2001) 14 *Australian Journal of Labour Law* 169.

[35] Ibid (Allens Arthur Robinson).

[36] Privacy New South Wales, 'Submission to the Australian Government Discussion Paper on Information Privacy and Employee Records' (29 April 2004), 3.

[37] Ibid.

privacy code's adjudicator. [38] Otherwise, the complaint process and available remedies are as described above. In accordance with the decision in *Seven Network (Operations) v MEAA***,** Mary would also be able to seek an injunction without first having to comply with the formal complaint process.

Although the Act provides an employee such as Mary with some effective redress where there is a breach of the privacy principles, this only applies in limited circumstances. The existence of statutory exceptions and the restrictions discussed earlier mean the Act is unable to address many of the issues that may arise through the use of monitoring, especially for employees in the private sector.

State/Territory Workplace Privacy Initiatives

Only New South Wales and Victoria have enacted specific workplace privacy legislation so discussion will initially focus on these measures. There is also a brief examination of information privacy provisions in the other states (including the Northern Territory) with respect to complaints by public sector employees. [39]

New South Wales

The *Workplace Surveillance Act* applies to monitoring activities whilst Mary is "at work" for her employer (or related business entity). [40] That is, when Mary is at her employer's workplace, (regardless of whether she is performing work for her employer), or at another place as long as she is actually performing duties for her employer at that location. [41] The Act applies to Mary regardless of whether she works in the public or private sector. [42] For present purposes, only the measures regulating overt surveillance

[38] 36(1A). The process must be relevant to the alleged breach. Sometimes the Privacy Commissioner acts as the adjudicator.

[39] The state based regimes generally apply only to the public sector. State based private sector employees can seek redress through the Commonwealth's *Privacy Act.*

[40] s 5.

[41] s 5(1)(a),(b).

[42] s 3 (definition of employee). The Act makes reference to the *Industrial Relations Act 1996* (NSW) which under section 5(1)(a) defines employee to mean "a person employed in any industry…."

activities are considered.

The Act does not seek to regulate the extent of surveillance, instead focusing on providing notice and the implementation of certain safeguards. Generally, the Act provides Mary protection by imposing the following obligations on her employer:

(a) Prior notification of surveillance activities
(b) Provision of a computer surveillance policy
(c) Prohibition of surveillance of non-work related activities in certain circumstances
(d) Prohibition of surveillance in certain parts of the workplace
(e) Restrictions on the disclosure of surveillance records

The major obligation imposed on Mary's employer is to provide her with prior written notice concerning surveillance activities. [43] Unless she agrees to a lesser period, Mary must receive notification 14 days before surveillance activities commence. [44] The notice must contain the following information: [45]

> (a) the kind of surveillance to be carried out (camera, computer or tracking), and
> (b) how the surveillance will be carried out, and
> (c) when the surveillance will start, and
> (d) whether the surveillance will be continuous or intermittent, and
> (e) whether the surveillance will be for a specified limited period or ongoing.

In accordance with the Act Mary's employer has established a computer use policy. [46] Mary was given a copy of the policy when she commenced work, and her employer should ensure she has sufficient awareness and understanding of its content. [47] The Act does not prescribe the manner in which this is to occur. However, it is reasonable to assume this may involve providing training or awareness sessions, making the policy

[43] s 10.
[44] s 10(2).
[45] s 10(4)(a)-(e).
[46] s 12(a).
[47] s 12(b).

available on the company's network, or placing it on a noticeboard where employee related notices are normally located.

Mary may also have grounds to complain if her employer has prevented delivery of her emails, or access to websites, unless such is in accordance with the company's email and Internet policy. [48] If Mary's employer prevents delivery of one or more emails, Mary should receive a "prevented delivery notice" as soon as practicable. [49] This is not required in the case of Spam, where an email (or its attachment) may damage the system, or it contains material that is "…menacing, harassing or offensive." [50] However, the Act prohibits the blocking of emails or access to websites "merely because" the email is sent by a trade union (or contains information about industrial matters) or the website accessed contains information on such matters. [51]

Mary's employer cannot monitor her activities whilst she is not "at work." [52] However, this does not apply to "…computer surveillance of the use by the employee of equipment or resources provided by or at the expense of the employer." [53] This may mean for example, where Mary's employer supplied her with a computer to use at home, all activities performed on this machine whether work related or otherwise, are subject to monitoring in accordance with the established policy.

Mary will also need to determine whether the CCTV cameras are operating in accordance with the Act. For example, the Act prevents her employer from installing hidden video cameras. [54] There must also be signs notifying the presence of cameras wherever video monitoring is taking place. [55] In addition, Mary's employer cannot conduct surveillance activities in change rooms, toilet or bathing facilities, or showers. [56]

---

48 s 17(1)(a). As with the computer surveillance policy Mary must be notified in advance in a manner whereby it is reasonable to assume she knows and understands how the policy applies.
49 s 17(1)(b).
50 s 17(2)(a)-(c).
51 s 17(4)(a),(b).
52 s 16(1).
53 s 16(1).
54 s 11(a).
55 s 11(b).
56 s 15.

Mary also needs to ensure her employer only uses or discloses information recorded as a result of conducting surveillance activities in accordance with the Act. Mary's employer can only use or disclose information from a surveillance record for a purpose related to her employment, or for legitimate business activities or commercial functions. [57] There exist exceptions for law enforcement agencies, civil or criminal proceedings, or "…to avert an imminent threat of serious violence to persons or of substantial damage to property." [58]

Under the circumstances, Mary's main avenue of complaint is where her employer has not provided the requisite notice in relation to video, email and Internet surveillance. She can also complain about any hidden cameras, or where cameras are not properly signposted.

Mary cannot complain about the monitoring of her emails or Internet usage in general, except if these were blocked simply because they related to trade union or industrial matters. Mary can also raise objections where the monitoring is in violation of the published policy. It is also likely her employer's use of the information acquired through monitoring for performance evaluation constitutes a legitimate business purpose.

Should Mary's employer breach the Act, she can institute proceedings for the imposition of a penalty (personal remedies are not available). [59] The Act provides a regulation may prescribe an offence for breaches of the Act punishable by a fine of up to five penalty units ($550). [60]

Mary cannot prevent her employer from reading her emails, or capturing images with cameras, or monitoring the websites she has visited, where the monitoring of these

[57] s 18(a).
[58] s 18(b)-(d).
[59] s 46(1)(d).
[60] s 44(3). A penalty unit is currently $110: s 17 *Crimes (Sentencing Procedure) Act 1999*.

activities is in accordance with the provisions the Act. [61] Beyond this, Mary has no redress, even if she believes the surveillance is intrusive, oppressive, or distasteful. Importantly, Mary's employer does not require her consent before implementing surveillance. [62] Also, as the definition of "at work" includes situations when an employee is in the workplace but not necessarily performing work, the Act allows Mary's employer to monitor her personal use of a computer during lunchtime or similar break. [63]

Thus, although the New South Wales Act affords Mary some level of protection, this is mostly through requiring the provision of notice. The Act does not limit the overall amount of surveillance an employer may conduct. This weakens the legislation's ability to effectively protect Mary's privacy rights or provide her with effective means of redress where a breach occurs.

Victoria

The Victorian *Surveillance Devices (Workplace Privacy) Act* 2006 is limited to preventing audio and video surveillance in specific areas of the workplace. The Act applies to Mary whether she is working for government or the private sector. [64] It allows Mary to lodge a complaint where her employer knowingly conducts such surveillance "…in a toilet, washroom, change room or lactation room in the workplace. " [65] It is also violation of the Act to communicate or publish a report of information acquired through conducting surveillance in these locations. [66]

Although the cameras used by Mary's employer have audio capabilities, this function is

---

61 With regard to reading emails see Jeremy Douglas-Stewart (ed.), *Workplace Surveillance Act 2005 (NSW): Handbook and Compliance Guide*: *the essential handbook for complying with workplace surveillance laws in NSW* (2005), [862].

62 Ibid [868]. Douglas-Stewart notes that if an employer wants to conduct surveillance other than for monitoring employees and does not want to provide notification, they can do so by obtaining the employee's consent.

63 Ibid [119].

64 s 9A.

65 s 9B(1).

66 s 9C(1).

not used. Therefore, under the circumstances, the Act is only relevant to her employer's use of silent video monitoring. There is however no regulation of video monitoring, other than where a camera is operating in a prohibited area (unless for instance the liquor licensing exception applies). [67] The lunchroom would not meet the definition of a prohibited area, nor would the operation of the cameras (even if the audio capability is used) in other areas of the workplace other than the prescribed locations.

The Act provides limited regulation of monitoring, and does not prevent Mary's employer installing and operating any number of cameras (hidden or otherwise) throughout the workplace. There is also no requirement to provide notice or any signs indicating surveillance is occurring. Even where a breach occurs, the Act does not provide Mary with access to personal remedies.

Reform Measures

The 2005 Victorian Law Reform Commission's report on workplace privacy includes a draft Bill (Workplace Privacy Act 2005). [68] I now assess Mary's options under this Bill. The proposed Act would apply regardless of whether Mary was a public servant or works for a private company. [69]

The overriding obligation under the draft Bill is that an employer should not engage in acts or practices that constitute an unreasonable intrusion of an employee's privacy when they are engaged in a work-related activity. [70] In order to determine such, Mary would firstly consider whether there was adequate information and opportunity for consultation regarding any proposed monitoring activity, in particular: [71]

> (i) the act or practice being considered and the reason for its proposed introduction; and
> (ii) the number, and categories, of workers likely to be affected by the act or practice; and
> (iii) the anticipated date of introduction of the act or practice; and

[67] ss 9B(2)(c), 9C(2)(c).
[68] Victorian Law Reform Commission, *Workplace Privacy Final Report* (2005), Appendix 5.
[69] s 3 (Definition of worker).
[70] s 8(1).
[71] s 5(a)(i)-(vi).

> (iv) the anticipated period during which the act or practice is proposed to be implemented; and
> (v) any alternative acts or practices considered and the reasons why they were not considered appropriate; and
> (vi) the safeguards to be used to ensure that the act or practice is conducted appropriately, having regard to the obligations in this Part;

Mary must be provided "…with a genuine opportunity to respond…" to what her employer has proposed, with the further obligation that her employer takes any issues raised by Mary "…into account when deciding whether or not to introduce the act or practice." [72] Mary's employer will also have unreasonably breached her privacy by conducting acts or practices in relation to work related activities: [73]

> (a) for a purpose that is not directly connected to the business of the employer; or
> (b) in a manner that is not proportionate to the purpose of the act or practice; or
> (c) without first taking reasonable steps to inform and consult with workers of the employer concerning the act or practice, in accordance with section 5; or
> (d) without providing adequate safeguards to ensure that the act or practice is conducted appropriately, having regard to the obligation in sub-section (1).

The above obligations also apply to third parties who assist an employer to conduct the monitoring. [74] An employer also requires authorisation to engage in acts or practices in relation to non-work related activities where such practices breach an employee's privacy. [75] There is also a prohibition on operating surveillance devices in toilets, change rooms, lactation rooms, or washrooms. [76] The Bill also allows for a prohibition on monitoring "…in any other prescribed circumstances." [77]

Therefore, Mary may have cause for complaint where adequate consultation has not occurred, or where the monitoring acquires her personal information that is unrelated to the company's business functions. Mary could also question monitoring activities she believes are not proportionate to the stated purpose for collection. For instance, this could include the number and placement of cameras, the amount of personal information collected through email and Internet monitoring, or similar concerns raised as part of the

[72] s 5(b)-(c).
[73] s 8(2)(a)-(d).
[74] s 8(3).
[75] s 9(1)(a).
[76] s 12(a).
[77] s 12(b).

consultative process. Mary can also ensure her employer has implemented appropriate safeguards.

Should Mary believe her employer is in breach of the legislation she would be able to lodge a written complaint with the Regulator. [78] Mary can also lodge a complaint on behalf of fellow workers (with their consent) if they are also affected by the alleged breach. [79]

The Regulator will make a preliminary assessment of Mary's complaint, and no later than 60 days after receipt decide whether to entertain it. [80] The Regulator may attempt informal resolution. [81] Should the Regulator decide to accept Mary's complaint (either in whole or in part) then if "reasonably possible" the matter moves to conciliation. [82]

Should the attempt to conciliate fail the Regulator can investigate the complaint under Division 4 or decide to take no further action. [83] Under Division 4 if the Regulator finds Mary's employer has breached her privacy, he or she may make a number of orders. Mary's employer may be required to cease the act or practice subject of the complaint, take specified actions to redress any loss or damage Mary has suffered, publish information with respect to the breach in a general circulation newspaper, or take action to protect the privacy of other workers. [84]

If conciliation or a ruling is inappropriate, Mary may request in writing that the Regulator refer her complaint to the Victorian Civil and Administrative Tribunal

---

78 ss 32(1)(a), 33(1). The Bill creates the new statutory office of Regulator (Part 8 Division 1). Apart from handling complaints, the Regulator issues codes of practice (both advisory to assist employers with their obligations and approved codes of practice for a workplace) and mandatory codes in relation to certain surveillance activities (ss 13-31).

79 s 32(3). A "representative body" having sufficient interest in the matter can also lodge a complaint on behalf of an employee(s): s 32(4).

80 ss 35(1), 37.

81 s 35(3).

82 ss 39(1)(a), 42(1).

83 s 46(1)(a). (Division 4 - Investigations, Rulings and Compliance Notices). This course of action is also available should the Regulator decide that conciliation is not appropriate: s 39(1)(b). If the Regulator decides neither conciliation nor a ruling are appropriate then he or she may decline to entertain the complaint further: s 39(1)(c).

84 s 47(4)(a)-(d).

("VCAT") for hearing. [85] The Regulator must acquiesce with her request. [86]

Should Mary successfully prove her complaint, VCAT can make a range of orders. These include restraining her employer from repeating or continuing the act or practice, order her employer redress any loss or damaged suffered, and award Mary monetary compensation up to a maximum of $100,000. [87] Mary's employer may also face civil and criminal penalties. [88] For example, where her employer breaches Mary's privacy by conducting surveillance in a toilet, change room, lactation room or wash room, Mary's employer may be ordered to pay a pecuniary penalty not exceeding $300,000 if her employer is a body corporate, or $60,000 otherwise. [89]

In summary, the Bill provides more substantial protection to employees such as Mary than existing measures in New South Wales or Victorian. The Bill also contains a comprehensive complaint process and the opportunity for Mary to seek a reasonable level of monetary compensation. If enacted the legislation would provide a useful adjunct to the general privacy framework in Victoria and address many of the concerns raised by employees over the use of electronic monitoring in the workplace.

State/Territory Information Privacy Initiatives

The absence of specific workplace privacy legislation outside Victoria and New South Wales means that in other jurisdictions Mary can seek to rely on information privacy laws. The definition of personal information in all of these measures is generally sufficient to encompass data acquired through electronic monitoring. [90]

---

85 s 40(1).
86 s 40(2).
87 s 60(a)(i)-(v).
88 Part 7.
89 ss 77(1)(c), 78(2)(b).
90 cl 7 Information Standard 42 (Qld); cl 3(1) *Cabinet Administrative Instruction to comply with Information Privacy Principles* (1989, 1992) (SA); s 4 *Information Act 2002* (NT); s 3 *Personal Information Protection Act 2004* (Tas); s 3 *Information Privacy Act 2000* (Vic). The definition in clause 7 of Information Standard 42 does not apply to Information Principle 6 (access) and Information Principle 7 (amendment). Personal information with respect to these two principles is limited to an individual's "personal affairs" as defined in the *Freedom of Information Act 1992*. The Tasmanian Act contains definitions of both "basic personal information" and "employee information."

Following below is a discussion of Mary's options under state and territory laws and administrative instruments. Although the New South Wales legislation is not canvassed (due to the existence of the *Workplace Surveillance Act*), because of the limited scope of the Victorian *Surveillance Devices (Workplace Privacy) Act*, there is discussion of Mary's rights under Victoria's *Information Privacy Act 2000*.

Queensland/ South Australia/Western Australia

Both Queensland and South Australia regulate information privacy by way of administrative instrument. [91] South Australia has also established a Privacy Committee whose role includes referring complaints to the appropriate authority. [92]

South Australia

As a South Australian public servant Mary has limited redress, as the Committee does not hear complaints from Crown employees in relation to their employment. [93] However, *Determination 2* issued under *Public Sector Management Act 1995* by the Commissioner for Public Employment outlines guidelines for agencies in relation to employees' personal files. [94] *Determination 2* recommends agencies refer to the IPP's (as outlined in the Cabinet Administrative Instruction) with respect to managing information contained in these files. [95]

Mary could also access her Department's internal grievance process, or seek external review thorough the Promotion and Grievance Appeals Tribunal if her complaint

---

91 Information Standard 42 (Qld); *Cabinet Administrative Instruction to comply with Information Privacy Principles* (1989, 1992) (SA).

92 *Proclamation of the Privacy Committee of South Australia* (1989).

93 cl 2(e) *Proclamation of the Privacy Committee of South Australia* (1989).

94 Office for the Commissioner for Public Employment, 'Determination 2: Recruitment and Employment of Non Executive Employees' (14 September 2001).

95 Ibid. See also Part II, *Cabinet Administrative Instruction to comply with Information Privacy Principles* (1989, 1992); Privacy Committee of South Australia, 'Privacy Committee Members Handbook Ver. 1.3' (February 2007), 11.

involves an administrative decision. [96] Even if Mary can lodge a complaint with the Privacy Committee, the Committee's powers are limited to referring her complaint to the appropriate authority. [97] Overall, the framework in South Australia provides little scope for Mary to address the issues of concern in her workplace. [98]

Queensland

If Mary believes her employer's conduct has breached the IPP's, she would initially lodge a written complaint with the privacy contact officer of the relevant agency. Mary should expect the agency would acknowledge her complaint within 14 days and seek finalisation within 60 days. [99]

If after this process Mary believes the issue requires further consideration, then she would need to apply in writing to the Director-General of the relevant department for an internal review of the decision. [100] If this still did not resolve the matter, Mary could seek to utilise the department's internal grievance process. If this was unsuccessful, she could lodge a complaint with the Public Service Commissioner or Ombudsman, or seek some form of administrative redress where applicable.

In accordance with the Queensland Government's *Use of the Internet and Electronic Mail Policy and Principles Statement,* Mary's department would have established a policy on employee use of email and the Internet. [101] The department also has a responsibility to provide Mary with training and other general information so that she will understand her responsibilities with respect to the operation of the policy. Thus,

---

[96] See Office for the Commissioner for Public Employment, 'Grievance Resolution: An Information Paper for Managers and Human Resource Practitioners' (March 1997).

[97] cl 2(e) *Proclamation of the Privacy Committee of South Australia* (1989).

[98] For further details regarding the operation of the Privacy Committee, see Government of South Australia, 'Annual Report of the Privacy Committee of South Australia - For the year ending 30 June 2007' (September 2007).

[99] See Queensland Government Privacy Website <http://www.privacy.qld.gov.au/complaint.htm> at 12 February 2008.

[100] Ibid.

[101] Office of the Public Service Commissioner, 'Use of Internet and Electronic Mail Policy and Principles Statement' <http//www.opsc.qld.gov/library/docs/resources/policies/internet_and_email_policy.pdf> at 2 June 2008.

monitoring conducted in accordance with the policy is probably unlikely to breach Mary's privacy.

These policies are important in regulating the use of information technology facilities and employees who breach such may face serious consequences. A recent case in the Industrial Relations Commission involved an employee appealing against his termination for breaching the agency's code of conduct and appropriate use of electronic communication systems policy. [102]

The Commission upheld the termination on the basis that Queensland Rail "…had a firm and well-publicised policy …" and the appellant had transmitted material which was in violation of that policy. [103] However, the Commission held that even though Queensland Rail's policy stated that a deliberate breach involving material of this nature would result in termination of employment, "…it ought not be assumed that the Commission would uphold the employer's right to apply the sanction of termination in all cases of deliberate breach regardless of the circumstances." [104]

Under Information Standard 38 the definition of "ICT facilities and devices" includes cameras. [105] Should Mary's department have in place a policy on the use of cameras, then Mary would need to refer to this with respect to her particular concerns regarding the use of CCTV in her work area. Otherwise, unless the cameras are operating in violation of the IPP's (in Information Standard 42), Mary would not have any grounds for complaint. [106]

Mary is also concerned about the use of her personal information for performance appraisal or other reasons. Again, if the Department's policy does not address this Mary

---

[102] *M. Wake v Queensland Rail* - PR974391 [2006] AIRC 663 (19 October 2006).
[103] Ibid [21]-[22].
[104] Ibid [23].
[105] Queensland Government Chief Information Officer, 'Use of ICT Facilities and Devices (IS38)' <http://www.qgcio.qld.gov.au/02_infostand/is38_print.pdf> at 2 June 2008.
[106] Queensland Government Chief Information Officer, Information Standard 42 (IS42) <http://www.qgcio.qld.gov.au/02_infostand/standards/is42.pdf> at 1 February 2008.

would need to ascertain whether the use or disclosure of her personal information in this manner violates Information Standard 42.

Mary has limited scope for redress as the focus of the Queensland system is on identifying and eradicating the errant conduct, (including apologising to the complainant), rather than on imposing fines or penalties. As with South Australia, there is little or no regulation of monitoring conduct beyond what is covered by individual policy statements and limited scope for a complainant to receive effective personal redress where a breach occurs.

Western Australia

A Bill to regulate the handling of personal information by the public sector is currently before the West Australian Parliament. [107] The definition of personal information includes where a person can be identified "…by reference to an identifier or an identifying particular such as a fingerprint, retina print or body sample." [108] An identifier is usually a number, but does not include situations where the identifier is only an individual's name. [109]

The Bill relevantly defines an interference with privacy in relation to personal information to include where a public organization contravenes its obligations in relation to the IPP's or applicable code of practice. [110] A code of practice contains any modifications made by an organization to the IPP's. [111] If there is an inconsistency between the code and the IPP's, the code prevails. [112]

[107] Information Privacy Bill 2007 (WA). The Bill also regulates the handling of health information, including where such information is held by private sector organizations: Pt 3.
[108] s 6(1)(b).
[109] s 4.
[110] ss 17, 65, 68(a),(c).
[111] s 57(1). Schedule 3 contains the IPP's.
[112] s 15(2).

The complaint process is similar to other states. Mary may complain directly in writing to the Commissioner about an alleged interference of her privacy. [113] The Commissioner may decide not to deal with Mary's complaint for a number of reasons. These include where Mary has not complained directly to the respondent and this is the appropriate course of action, or where after receiving the complaint from Mary, the respondent agency has or is dealing with the matter adequately, or has not had adequate opportunity to do so. [114]

Mary's complaint may be resolved through conciliation, and a documentary record of the agreement between the parties produced. [115] In circumstances where the Commissioner decides not to proceed with the complaint, [116] or the matter remains unresolved after conciliation, [117] Mary can require the matter be referred to the State Administrative Tribunal ("Tribunal"). [118]

If Mary can substantiate her complaint (or any part thereof) the Tribunal may make one or more orders. For example an order restraining Mary's employer from continuing with the interference to her privacy, that her employer redress any loss or damage suffered, or that her employer pay Mary compensation up to a maximum of $40,000. [119] The Tribunal may also find Mary's complaint substantiated but decline to take any further action. [120] Mary can also appeal the Tribunal's decision. [121]

Mary would need to demonstrate the monitoring breaches the IPP's. An approved code of practice may modify the IPP's in relation to "any specified personal information" or "any specified activity" thus Mary would need to consider whether any such changes might impact on her opportunity for complaint. [122] Generally, Mary's opportunities for

[113] ss 69(a), 72(1)(a).
[114] s 73(1)(a)-(f).
[115] s 80(1).
[116] s 73(1).
[117] s 85(1).
[118] s 75(1).
[119] s 90(1)(b)(i)-(iii).
[120] s 90(1)(c).
[121] s 93(1).
[122] s 57(2)(a),(b).

seeking redress under the proposed Bill are similar to existing information privacy measures in other jurisdictions.

Northern Territory

As a public employee in the Northern Territory, Mary would initially lodge her complaint directly with the offending agency. [123] Complaints can be for a breach of the IPP's or where an agency "…has otherwise interfered with the person's privacy." [124] If Mary's discussions with the agency prove unsuccessful, she could lodge a written complaint with the Information Commissioner. [125]

Within 90 days of receiving Mary's complaint the Commissioner must decide whether to accept or reject it and notify her accordingly. [126] If the Commissioner accepts the complaint, an investigation must commence. [127] Where sufficient prima facie evidence to substantiate Mary's complaint exists, the matter moves to mandatory mediation, otherwise the Commissioner must dismiss the complaint. [128]

If mediation or other attempts at resolution fail to resolve Mary's complaint, the Commissioner conducts a hearing. [129] If after the hearing, the Commissioner upholds Mary's complaint he or she may make an order. Mary's employer may be ordered to refrain from the conduct complained of, correct Mary's personal information, attach a statement from the Commissioner to her personal information, where appropriate pay Mary monetary compensation for any loss or damage suffered up to a maximum of $60 000, or make an apology. [130]

[123] s 104(2)(a) *Information Act 2002* (NT).
[124] s 104(1).
[125] ss 104(1), 105(a).
[126] s 106(1).
[127] s 110(1).
[128] s 110(3)-(5).
[129] ss 111(1), 113(1), 121-28.
[130] s 115 (4). Such orders are also available should mediation or other agreement resolve the matter: s 112.

An advantage of the legislation is that it allows complaints about breaches of privacy other than in relation to the IPP's. This means Mary can complain about the general use of cameras, where the monitoring collects excessive amounts of her personal information, or if the information is used in an inappropriate manner. Importantly the Act also allows the possibility for Mary to receive a reasonable level of monetary compensation should a serious breach occur.

Tasmania

Tasmania has the most recently enacted legislation. [131] Under the *Personal Information Protection Act* Mary must first raise any concerns she has about the monitoring contravening any of the personal information protection principles with the relevant agency. [132] In Tasmania, the Ombudsman has responsibility for hearing complaints. If the matter remains unresolved after negotiation with the offending agency, Mary can complain either verbally or in writing to the Ombudsman. [133]

The Ombudsman may conduct preliminary assessment of the matter to decide whether to entertain the complaint. [134] The Ombudsman may also refer Mary's complaint to the State Service Commissioner or other relevant authorities, but must first consult with the other organization and Mary, and consider their views on this course of action. [135]

If the Ombudsman accepts Mary's complaint for investigation, such proceeds in accordance with Division 3 of Part II of the *Ombudsman Act 1978* (Tas). [136] On completion of the investigation, should the Ombudsman find Mary's employer has breached the privacy principles, the Ombudsman may make any recommendation

[131] *Personal Information Protection Act* 2004 (Tas).
[132] s 18(1)(a),(2), sch 1. Agencies and other relevant organizations are called "personal information custodians" and include a public sector body, a council, the University of Tasmania, and third parties who are engaged by personal information custodians to collect personal information: s 3.
[133] s 18 (1),(3).
[134] s 19(1).
[135] s 20.
[136] s 21(1).

appropriate to the subject matter of the complaint. [137]

One specific problem Mary might face arises from the fact that certain employee information is exempt from the provisions of the Act. [138] This could potentially include information acquired through monitoring. The exemptions have the effect of allowing agencies more flexibility when handling employees' personal information. For example, the restraint against collecting information from persons other than the individual where "…it is reasonable and practicable to do so..." does not apply. [139] In addition, where an agency collects information from a third party it does not need to take reasonable steps to inform the individual of: [140]

> (a) its identity and how to contact it;
> (b) the individual's right of access to the information;
> (c) the purposes for which the information is collected;
> (d) the intended recipients or class of recipients of the information;
> (e) any law that requires the information to be collected;
> (f) the main consequences for the individual if all or part of the information is not provided.

Under the exemption, agencies can also assign employees an individual identifier, (or adopt an existing identifier assigned by another agency) absent the constraint that such action is necessary for the performance of the agency's functions. [141] Other requirements, for instance, with respect to collecting sensitive information, (such as requiring consent) also do not apply to employee information. [142]

Mary cannot prevent the use of information acquired through monitoring for performance appraisal or disciplinary matters (as long as such actions are conducted in accordance with the provisions of the Act), nor restrict the collection of sensitive personal information. Overall, the exemptions may seriously affect Mary's ability to effectively redress intrusions caused by monitoring.

---

[137] s 22(1)(b).
[138] s 10. Clauses 1(4) and (5), 7 and 10 of Schedule 1 (Personal Information Protection Principles) do not apply to "employee information." This includes such things as pay, hours, and conditions, details about performance or conduct, termination, and union membership: s 3.
[139] cl 1(4) sch 1.
[140] cls 1(5), 1(3) sch 1.
[141] cl 7 sch 1.
[142] cl 10 sch 1.

As with the measures discussed earlier Mary has little recourse with respect to overall monitoring activity unless this interferes with the privacy principles. The focus of the legislation is on the making of recommendations, thus even where Mary can demonstrate a breach, she cannot pursue personal or other remedies. The Act's lack of specific provisions with respect to workplace monitoring, the exemptions detailed above, and the existence of a monitoring policy, mean Mary is unlikely to make much progress with respect to her concerns.

Victoria

By comparison with the jurisdictions referred to earlier, the Victorian *Information Privacy Act 2000* provides more substantive mechanisms to assist the resolution of workplace privacy issues. To begin with, there are broad similarities with other states in respect to the complaint process. Mary may lodge a written complaint directly with the Victorian Privacy Commissioner concerning any acts or practices that constitute an interference with her privacy. [143] The Commissioner must notify Mary within 90 days of lodgement if he or she decides not to proceed with the complaint. [144]

If Mary's complaint is accepted, the Commissioner must attempt resolution by conciliation if possible, [145] and if successful, the parties may conclude a conciliation agreement. [146] If conciliation is unsuccessful, Mary may request that the Commissioner refer the matter to VCAT for determination. [147] The Commissioner must accede to this request. [148] VCAT may make a number of orders including that Mary's employer pay her up to $100,000 in compensation for any loss or damage suffered. [149]

[143] s 25(1) *Information Privacy Act 2000* (Vic). The Commissioner may decline a complaint if it has not been first directed to the offending agency: s 29(1)(c).
[144] s 29(1).
[145] s 33(1).
[146] s 35(1).
[147] s 37(3). Mary has 60 days to inform the Commissioner the matter is to be referred to Tribunal. Mary can also seek this course of action if the complaint is initially declined: s 29(2).
[148] s 37(4).
[149] s 43(1)(a)(iii).

The following decisions may provide Mary with some guidance as to how VCAT may address her concerns. In *Complainant L* an employee's email messages sent to and from a work email account were automatically copied to his Manager without his knowledge or consent. [150] The facts gave rise to issues covered under IPP 1(Collection) and IPP 4 (Data Security). [151] Successful conciliation resulted in the employer apologising to the complainant, agreeing to review its email policy (including examination of consistency between email, Internet and privacy policies), and to advise specified third parties of its failure to inform the Complainant of its monitoring activities. [152]

Ng v Department of Education involved the use of CCTV footage to assess a teacher's classroom management abilities. [153] Mrs Ng was a teacher in a state senior secondary college and taught a number of subjects including information technology and business management. [154] The school installed CCTV cameras in a number of locations including the computer rooms. [155] The cameras were required in the computer rooms because the intention was that students would access these rooms outside normal class times and without direct supervision. [156] Ng regularly took classes in a computer room. [157]

Because of concerns over Mrs Ng's classroom management abilities in light of allegations of unruly behaviour by her students, [158] the Principal reviewed CCTV footage of the incident and sent Mrs Ng a letter containing details of the allegations. [159] Later, at a meeting with Ng and the Principal, the Assistant Principal and a union representative also viewed the tape. [160] Mrs Ng complained to the Commissioner that the school's actions with respect to the CCTV footage breached the IPP's. [161]

---

[150] *Complainant L v Tertiary Institution* [2004] VPrivCmr6, 1.
[151] Ibid.
[152] Ibid 2.
[153] *Ng v Department of Education* [2005] VCAT 1054 (Macnamara, Deputy President).
[154] Ibid [1].
[155] Ibid [4].
[156] Ibid. There were no cameras in the ordinary classrooms.
[157] Ibid [5].
[158] Ibid [5]-[7].
[159] Ibid [8]-[9].
[160] Ibid [14]-[15]. The Principal also allowed two teachers to view the footage but had no recollection of showing it to a former student: [16].
[161] Ibid [26].

The Victorian Department of Education had published guidelines for the use of CCTV in schools, which amongst other things prohibited its use for monitoring individual work performance, and providing without appropriate approval, images recorded in schools to third parties. [162] A representative from the Security Management Unit of the Education Department gave evidence that, as schools were self-governing, the school could choose to follow the actions it had taken without regard to the guidelines. [163] Mrs Ng argued the guidelines were rules and thus prevented using the footage to monitor her classroom performance. [164] Mrs Ng also stated the purpose for installing CCTV was detecting vandalism and graffiti, and that as the guidelines made no distinction between live viewing and viewing recorded footage, the Principal had violated the guidelines both when initially viewing the footage and again when he showed it to the other teachers. [165]

VCAT held the video footage was personal information. [166] VCAT also determined the use of the CCTV cameras did not breach the IPP's because it was reasonably required and ancillary to the functions of operating a school, there was no illegality involved in the installation and use of such equipment, and that there were notices providing adequate warning that video surveillance was occurring in that area. [167]

The purpose for collecting the information was to monitor inappropriate conduct by students. [168] The secondary purpose for reviewing the video was to ascertain how Mrs Ng managed such behaviour. [169] VCAT also held there is a clear link between reviewing Mrs Ng's classroom management abilities with respect to unruly behaviour, and that behaviour itself. [170] VCAT dismissed Mrs Ng's complaint. [171]

---

[162] Ibid [46]-[51].
[163] Ibid [51]. The school had not sought express permission as required under the policy before providing the footage to third parties: [50]. However the Principal and the manager of the Department's Conduct and Ethics Branch gave evidence that they believed the guidelines were binding rules: [53].
[164] Ibid [53-4]. Although the Department's Information Privacy policy refers to the IPP's, it states that any personal or health information collected would be used to investigate incidents in schools and defend legal actions:[51].
[165] Ibid [53], [55].
[166] Ibid [39].
[167] Ibid [22], [85]-[87].
[168] Ibid [93].
[169] Ibid [94].
[170] Ibid.

This decision is noteworthy for a number of reasons including its application of the IPP's to the use of CCTV. VCAT also noted that an infringement of the CCTV guidelines was not necessarily an infringement of the IPP's, that the guidelines prescribed no penalty for breach, and that VCAT had no power to enforce them. [172]

This (and the decision discussed earlier involving Queensland Rail) appears to indicate there exists some degree of uncertainty regarding the applicability and enforceability of such policies. As government departments (and an increasing number of private companies) have implemented procedures regulating the use of information and communication technology equipment by employees, it is imperative that this issue be resolved, preferably through legislative action.

Although many of the same limitations apply with respect to linking breaches to the IPP's, the Victorian legislation offers a more comprehensive approach to determining privacy breaches with a reasonable capacity for application to workplace privacy issues. In addition, a wider range of remedies including monetary compensation is available.

Information Privacy Laws and Workplace Privacy

Information privacy laws are a useful adjunct to privacy protection, but are generally insufficient to deal with the complexities raised by the use of electronic monitoring in the workplace. As most of the measures only apply to actions by government agencies, they offer little redress if Mary is in the private sector. As with the Commonwealth's *Privacy Act*, the state based statutes mostly only apply where there is a breach of the IPP's. With the exception of Victoria and the Northern Territory, there is little opportunity for employees to seek substantive personal remedies.

In addition, the complaint process often requires the aggrieved party to attempt to resolve the matter with the offending agency. In many instances this will be the person's

[171] Ibid [99].
[172] Ibid [74-5].

employer. Depending on the extent and nature of the alleged breach, this may not be the most appropriate course of action for either party.

It is important to appreciate though that information privacy laws have made a significant contribution to the protection of privacy in Australia. [173] Furthermore, for many employees these measures may be the only effective means to seek redress where a breach occurs.

The Tort of Invasion of Privacy - A Possible Remedy?

Apart from legislative and other measures of protection outlined earlier, given some recent decisions, it is theoretically possible for Mary to seek a remedy at common law. The attraction of this cause of action is its flexibility, that it applies to both private and public employees, and importantly offers an opportunity to obtain damages. [174] The few decisions to date which have applied the tort have addressed differing types of intrusions. For instance, *Doe v ABC* involved unjustified publication of the plaintiff's personal information similar to the tort of unreasonable publicity in the United States. [175] The New Zealand Court of Appeal found a similar breach in *Hosking v Runting.* [176] Whereas in *Grosse v Purvis*, the defendant's conduct amounted to unlawful stalking under the *Criminal Code* thus constituting an invasion of the plaintiff's privacy. [177]

In *Grosse* Skoien SJ outlined the following cumulative test that could be applied to determine whether a breach of privacy has occurred: [178]

---

[173] See David Lindsay, 'An exploration of the conceptual basis of privacy and the implications for the future of Australian privacy law' (2005) 29 *Melbourne University Law Review* 131, 133.

[174] "…that the invasion, or breach of privacy alleged here is an actionable wrong which gives rise to a right to recover damages according to the ordinary principles governing damages in tort." *Doe v ABC* & Ors [2007] VCC 281, [157] (Hampel J).

[175] *Restatement (Second) of Torts* (1977), § 652D (unreasonable publicity given to the other's private life).

[176] *Hosking v Runting* [2005] 1 NZLR 1, [68]. See also John Burrows, 'Invasion of privacy – Hosking and Beyond' (2006) 3 *New Zealand Law Review* 389.

[177] *Grosse v Purvis* (2003) Aust Torts Reports ¶81-706, [420] (Skoien SJ).

[178] Ibid [444]. His Honour noted that in formulating the test it was "…not my task nor my intent to state the limits of the cause of action nor any special defences other than is necessary for the purposes of this case." See also Paul Telford, 'Gross v Purvis: its place in the common law of privacy' [2003] PLPR 36.

(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,
(d) and which causes the plaintiff detriment in the form of mental psychological or emotional harm or distress or which prevents or hinders the plaintiff from doing an act which she is lawfully entitled to do

The above elements share some similarity with the United States tort of unreasonable intrusion upon the seclusion of another (discussed later). [179] There are however some important differences. Elements (a) and (b) change the intention requirement to cover only the intrusive act (rather than both the act and the result) which may "…allow for the possibility of culpable intrusions which are accidental, provided the intruding act itself is intended. [180] His Honour also added a further element (d) requiring that there exist psychological and emotional detriment preventing the plaintiff engaging in lawful acts. [181]

The monitoring activities engaged in by Mary's employer may meet elements (a) and (b). The problem for Mary is establishing the conduct complained of is highly offensive to a reasonable person, and that the monitoring has caused the detriment required by element (d). It would appear only the most intrusive forms of monitoring (such as where hidden cameras are placed in changing rooms or similar), or where particularly sensitive personal information unrelated to any of her employer's business activities was captured through monitoring Mary's emails, Internet or other communications, may satisfy elements (c) and (d). The mere presence of cameras or the conducting of routine monitoring (especially when her employer has detailed policy guidelines) would probably be insufficient grounds on which to base an action in tort.

Applying the test from *Grosse* also raises a number of other questions, including whether negligent conduct or wilful blindness on the part of the defendant is sufficient,

[179] *Restatement (Second) of Torts* (1977), § 652B.
[180] Des Butler, 'A Tort of Invasion of Privacy in Australia?'(2005) 29 *Melbourne University Law Review* 339, 359. These elements essentially replace the following wording from Intrusion "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another…."
[181] See discussion of this case in Butler, above n 180, 357-60.

the type of damage required, and what defences will be available. [182] In addition, the problem of establishing an objective expectation of privacy in the workplace has proved extremely problematic for plaintiffs in the United States. This is also likely to present a problem for Australian workers like Mary. Current decisions do not provide sufficient guidance as to whether Mary would succeed in an action at common law, however it would appear she would face significant difficulties.

The United States

Pauline Kim notes that the legal analysis of workplace intrusions in the United States focuses on the invasiveness of individual technologies, reflected by the various statutory measures at the federal and state level that regulate only particular types of invasions, rather than intrusions in general. [183] As such, there are a number of statutory, constitutional and common law avenues available to Mary.

Constitutional Protection under the Fourth Amendment

Monitoring may violate the Fourth Amendment. In order to assert her Fourth Amendment rights Mary would need to be a public sector employee (either federal or state). Mary must also demonstrate she has a subjective expectation of privacy which society considers objectively reasonable. Following the standard enunciated in *O'Connor v. Ortega*, this will be determined on a case-by-case basis involving balancing her legitimate expectation of privacy, against the operational realities of the workplace. This involves the consideration of a number of factors, including whether Mary has her own office, the access other people have to her work area, and the need for Mary's supervisor to retrieve her information for work related purposes.

Mary works in an open plan office area and this can be determinative of whether a

[182] Mark Sneddon and Riccardo Troiano, 'New tort of invasion of privacy and the Internet' (2003) 6(6) *Internet Law Bulletin* 61, 62.
[183] Pauline T. Kim, 'Privacy Rights, Public Policy, and the Employment Relationship' (1996) 57 *Ohio State Law Journal* 671, 674.

reasonable expectation of privacy arises. [184] Overall, Mary's expectation of privacy at work will be less than at home. [185]

Video Monitoring

Mary is concerned over her employer's use of video monitoring (including the possible deployment of hidden cameras). The Court in *Vega- Rodriguez v. Puerto Rico Telephone Company* found no violation of the Fourth Amendment where an employer notified its workforce in advance about the use of silent video cameras and disclosed the camera's field of vision. [186] The Court also held that surveillance of activities displayed openly does not constitute a violation simply because the activities are observed electronically rather than by physical observation. [187]

In *Nelson v. Salem State College*, a hidden video camera captured the plaintiff as she changed clothes and applied sunburn medication to her neck and upper chest area. [188] Nelson's office was accessible to other employees and volunteers (even when the door was locked as they had keys) and to members of the public. [189] The office also had a large window that allowed anyone passing by full view of its interior. [190]

Although the operation of 24 hour video surveillance of the entire office was "unnecessarily broad" to investigate alleged criminal activity after hours, the operation of the camera did not raise the concerns expressed in *Vega-Rodriguez v. Puerto Rico*

[184] *Vega-Rodriguez v. Puerto Rico Telephone Company*, 110 F.3d 174, 180 (1st Cir. 1997) (Selya J). An employee can have an objectively reasonable expectation of privacy where they have exclusive use of an office and they secure such to prevent forcible entry by others outside work hours: *United States v. Taketa*, 923 F.2d 665, 673 (9th Cir. 1991) (Beezer J).

[185] See fn 6 *United States v. Leary*, 846 F.2d 592, 597 (10th Cir. 1988) (Anderson J).

[186] *Vega-Rodriguez v. Puerto Rico Telephone Company*, 110 F.3d 174, 180, 182 (1st Cir. 1997) (Selya J). Although the Court did caution against covert surveillance involving the use of clandestine cameras (dicta fn 5).

[187] Ibid 181(Citing LaFave).

[188] *Nelson v. Salem State College*, 446 Mass. 525, 526 (2006) (Ireland J). The camera was in a light fixture on the office's rear wall. The plaintiff's activities occurred in the area where the camera was operating, however none of the recordings preserved contained any images of the plaintiff engaging in such. Once the plaintiff became aware of the use of the hidden camera she commenced the litigation: (529-30).

[189] Ibid 534.

[190] Ibid 534-5.

Telephone Company. [191] Even though the plaintiff did not have notice of the monitoring, the facts of the case, including the public nature of the work engaged in by the organization, combined with "…the ready visual and physical access that was afforded the public, all employees (including management) and volunteers … abrogated any objectively reasonable expectation of privacy." [192]

In *Thompson v. Johnson County Community College*, the plaintiffs (all security officers) claimed their employer had conducted video surveillance in their locker room. [193] The locker room was also a storage area, as well as containing heating and air-conditioning equipment. [194] Individuals other than the plaintiffs used the room, and access was not restricted by key or otherwise to persons entering the room for legitimate business reasons. [195] Although Courts have previously found a reasonable expectation of privacy in lockers used to store personal items, this has not extended to areas adjacent to the lockers. [196] Although few people other than the plaintiffs entered the room, the locker area was accessible to anyone who came into the room, thus the plaintiffs could not demonstrate a reasonable expectation of privacy in the locker area. [197]

In *Williams v. City of Tulsa* the court held surveillance conducted in the restroom was subject to Fourth Amendment protection as this area was one in which the plaintiffs could demonstrate an objective expectation of privacy. [198] Additionally, in *Vega-Rodriguez v. Puerto Rico Telephone Company* the Court stated that installing a camera in a restroom "…would raise a serious constitutional question." [199]

---

[191] Ibid 535.
[192] Ibid 536.
[193] *Thompson v. Johnson County Community College*, 1997 U.S. App. LEXIS 5832, *2 -3 (Porfilio J). The plaintiffs claimed the camera used was also capable of audio recording, however the defendants disputed this: (fn 1).
[194] Ibid *4.
[195] Ibid *4-5.
[196] Ibid *6-7.
[197] Ibid *7.
[198] *Williams v. City of Tulsa***,** 2005 U.S. Dist. LEXIS 37889, *11-12 (H. Dale Cook J). The plaintiffs also alleged surveillance was conducted in several offices, the maintenance and weld shops, the lift station, and some open areas of the workplace.
[199] *Vega-Rodriguez v. Puerto Rico Telephone Company*, 110 F.3d 174, 182 (1st Cir. 1997) (Selya J). (Citing *People v. Dezek*).

Given Mary is aware of her employer's use of silent video surveillance, the general operation of cameras in the workplace is unlikely to raise issues with respect to her Fourth Amendment rights. Mary could however seek to rely on *Vega-Rodriguez* regarding the use of hidden cameras, and argue the case law involving video surveillance in restrooms should apply to the camera in the lunchroom.

Other Monitoring Activities

As Mary's employer has implemented a monitoring policy, it is less likely the monitoring of her email and Internet usage constitutes a violation of the Fourth Amendment. There are a number of decisions involving the possession of inappropriate or unlawful material that have discussed the applicability of computer use policies. Discussion of several of these follows below. [200]

In *United States v. Thorn*, the defendant, who worked for a state government agency, had allegedly distributed non-work related emails and used his work computer to access adult websites in violation of agency policy. [201] The agency's communication policy prohibited personal use of the email system and access to inappropriate emails, electronic documents and pictures. [202] The policy also clearly stated that employees did not have any personal privacy rights with respect to the use of the computer systems, and acknowledged the agency had a right to access and audit system usage. [203] Thorn was aware of the policy and had provided a written acknowledgement of such when he initially requested access to the system. [204] The Court held the above factors meant Thorn did not have a reasonable expectation of privacy with respect to the use of his work computer or its contents. [205]

[200] Most of the cases discussed involve an appeal against the denial by the trial court to allow the defendant's motion to suppress evidence. Entering a conditional guilty plea after sentence and judgment has been imposed allows the defendant the right to appeal the denial of a motion to suppress evidence that the defendant argues was obtained in violation of their Fourth Amendment rights: see *United States v. Thorn*, 375 F.3d 679, 681 (fn.2) (8th Cir. 2004) (Bowman J).
[201] Ibid 681.
[202] Ibid 682.
[203] Ibid.
[204] Ibid 682-3.
[205] Ibid 683.

Similarly, in *United States v. Angevine*, police located unlawful images on a computer used by a staff member at Oklahoma State University. [206] The University had a detailed computer use policy that included a prohibition on accessing inappropriate material, and also informed users that it reserved the right to scan and view files or software on university computers, or which passed through the network, and would do so on a periodic basis. [207] The policy also stated that where there is suspicion an employee is violating federal or state law, and an internal investigation is required, system administrators may monitor all files and activities of that user. [208]

The Court found Angevine did not have a reasonable expectation of privacy regarding the material he downloaded onto his work computer because this activity was in violation of the University's policies and procedures. [209] The computer was owned by the University and issued to Angevine for work related reasons, thus in such circumstances he should have expected these polices would constrain his expectation of privacy. [210]

However, Mary may be able to rely on the decision in *Haynes v. Office of the Attorney General*. [211] An Office of the Attorney General ("AG's Office") staff member told Haynes during orientation that his work computer contained a private and public file, and that no one would have access to any personal information he placed in his private file. [212] The computer policy also appeared briefly on each computer when a user switched on the machine. [213] This included informing users to consult with their superiors in relation to acquiring all policies and procedures, that limited personal use

[206] *United States v. Angevine*, 281 F.3d 1130, 1132 (10th Cir. 2002) (Brorby J).
[207] Ibid 1132.
[208] Ibid 1133. There was also a "splash screen" displayed on all computers at startup which stated that there was no right of privacy in emails (except as provided by law) and that the university had the right to inspect emails without notice at any time to protect its business interests.
[209] Ibid 1134.
[210] Ibid 1135. The court also held that the images were not in Angevine's immediate control (he had attempted to delete them and the police experts had later accessed them from his computer) and he took no actions consistent with private ownership by downloading images to a University owned computer that was accessible by third parties.
[211] *Haynes v. Office of the Attorney General*, 298 F. Supp. 2d 1154 (D. Kan. 2003) (Rogers J). This case did not involve the acquisition of unlawful material.
[212] Ibid 1157.
[213] Ibid 1158.

was acceptable, and although users had no expectation of privacy when using the system, there existed a prohibition against intentionally accessing a user's email unless "…authorized by computer use procedures." [214]

The AG's Office terminated Haynes appointment before he was able to copy all of his personal files from the computer. [215] Later employees of the AG's Office retrieved information from his computer including his personal emails. [216] The Court held Haynes had a subjective expectation of privacy in the private information on his computer. [217] Even though the policy stated employees had no expectation of privacy, other information in the policy combined with the oral representations made during the orientation, meant that his expectation of privacy in his private files was objectively reasonable. [218]

The Court considered a number of factors in reaching this conclusion. These included the existence of private/public areas of the computer, that access to the computers was by way of password, that employees could engage in limited private use, that the policy prohibited the intentional access of another person's emails, and that there was no evidence anyone from the office had monitored communications or viewed employees' files previously. [219]

However a number of hurdles remain. Even if Mary used her own computer equipment, this would not necessarily mean she could establish the necessary expectation of privacy.

In *United States v. Barrows*, the plaintiff (Barrows) brought his own laptop from home leaving it in an open work area shared with another employee. [220] Barrows connected the

[214] Ibid.
[215] Ibid.
[216] Ibid.
[217] Ibid 1161-2.
[218] Ibid 1162.
[219] Ibid 1162.
[220] *United States v Barrows*, 481 F.3d 1246, 1247 (10th Cir. 2007) (McConnell J).

laptop to the office network. [221] Barrows did not password protect the machine or otherwise secure it, or attempt to exclude other employees from using it and left it on at all times. [222] Child pornography was discovered on the laptop when the machine was being examined in relation to problems being experienced with the office computer. [223]

Barrows pled guilty to the pornography charges, however appealed the district court's denial of his motion to suppress. [224] In finding Barrows did not have a subjective expectation of privacy in his laptop, the Court noted that ownership in itself is insufficient to ground such expectation, particularly where the machine is used for business purposes. [225] More importantly, Barrows failed to take reasonable steps to maintain privacy in the machine, including leaving it constantly switched on, not assigning a password, and not limiting access by others. [226]

Even in circumstances where Mary is able to demonstrate some expectation of privacy in the contents of her computer, the search may still not violate her Fourth Amendment rights. This could occur for example, where the search is by her supervisor to retrieve work related material, or to obtain evidence of misconduct. [227]

In light of the surrounding circumstances, it is unlikely Mary could establish a violation of her Fourth Amendment rights with respect to monitoring of her email and Internet, or the use of such data for performance monitoring or similar business related reasons. As noted in *Vega- Rodriguez* "…employees must accept some circumscription of their liberty as a condition of continued employment." [228] However, if Mary can establish the monitoring is unconstitutional, then she may take civil action for damages or other

[221] Ibid.
[222] Ibid.
[223] Ibid.
[224] Ibid 1248.
[225] Ibid 1249.
[226] Ibid.
[227] *O'Connor v. Ortega*, 480 U.S. 709, 725-6 (1987) (O'Connor J, Rehnquist CJ, White, Powell JJ). There must be reasonable suspicion that the search will find evidence of misconduct.
[228] *Vega-Rodriguez v. Puerto Rico Telephone Company*, 110 F.3d 174, 180 (1st Cir. 1997) (Selya J) (Citing *INS v. Delgado*).

appropriate remedy. [229]

United States Federal Statutes

The Privacy Act

The *Privacy Act of 1974* regulates the collection and handling of personal information by federal government agencies. [230] Therefore, Mary would need to work in the federal public sector in order to seek redress. The complaint process involves taking civil action in a district court. [231]

A number of factors limit Mary's chances of seeking effective redress under the Act. Firstly, the monitoring information acquired must form part of her record held by the agency in question. Even so, Mary may not have access to all information held, only such that meets the system of records definition.

Similar to its Australian counterpart, redress is generally only available where there is a violation of the privacy principles as they relate to record handling procedures. An additional potential impediment is that Mary must show actual damage. This could pose somewhat of a problem given the nature of some monitoring technologies, for although Mary may for example, suffer emotional harm because of a breach, a court may not consider this sufficient to obtain a remedy.

It is therefore unlikely this legislation would provide a suitable avenue for Mary to address her concerns over monitoring at her workplace. However, it has been held the Act does not pre-empt the common law with respect to federal government information, thus Mary could pursue other avenues if she is unsuccessful in seeking redress under the

[229] 42 U.S.C. § 1983 (2006). This statute allows an individual to take civil action for the deprivation of their Constitutional rights, privileges or immunities.
[230] *Privacy Act of 1974*, Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C § 552a (2006)).
[231] § 552a (g)(1).

Act. [232]

The Electronic Communications Privacy Act

The *Electronic Communications Privacy Act of 1986* ("ECPA") is available to employees in both the public and private sector. [233] The Act relevantly contains the *Wiretap Act* (which regulates interceptions) and the *Stored Communications Act* ("*SCA*") - which regulates access to communications stored on servers and similar locations. Depending on the circumstances Mary can seek protection under either or both of the constituent elements. The ECPA does not prescribe a particular process for seeking redress other than taking action through the courts.

Mary has no recourse under the *Wiretap Act* in relation to her employer's use of silent video monitoring. [234] As noted in Chapter Two, federal law is inconclusive with respect to the applicability of the Act "…to targeted silent video surveillance..." in certain circumstances. [235] It may be possible for Mary to pursue an action under the ECPA if she can demonstrate the requisite expectation of privacy. It is unlikely however that this would be the case with respect to use of cameras generally, except perhaps if the cameras were located in areas such as bathrooms or locker rooms.

With respect to the monitoring of her emails and use of the Internet, to demonstrate a violation of the *Wiretap Act*, Mary must prove her employer intentionally intercepted (or attempted to intercept) her electronic communication, such communication affecting

---

[232] See *Alexander v. Federal Bureau of Investigation*, 971 F. Supp. 603, 605, 610-11 (DC. Cir. 1997) (Lamberth J). Known as "Filegate" this case involved allegations of improper handling by the FBI of records of former employees of the Reagan and Bush administrations. The claims involved alleged breaches of the *Privacy Act* and common law invasion of privacy. The Court was required to address the issue of the intersection of the Act and the common law when one of the defendants argued that the *Privacy Act* pre-empts the tort of invasion of privacy.

[233] *Electronic Communications Privacy Act of 1986*, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510-2522, 2701-2712 (2006)).

[234] *Thompson v. Johnson County Community College*, 1997 U.S. App. LEXIS 5832, *3 (Porfilio J).

[235] Robert D. Bickel, Susan Brinkley and Wendy White, 'Seeing Past Privacy. Will the Development and Application of CCTV and Other Video Security Technology Compromise an Essential Constitutional Right in a Democracy, or Will the Courts Strike a Proper Balance?'(2003) 33 *Stetson Law Review* 299, 315-6 (and cases cited therein).

"interstate or foreign commerce,…." [236] Alternatively, Mary may have a remedy under the *SCA* where her employer has intentionally gained unauthorised access to her stored electronic communications. [237]

Even where Mary can prove her employer's monitoring activities have resulted in an unauthorised interception or unauthorised access of her communications, her employer will have a complete defence if the monitoring activities fall within one of the exceptions. For example, even where Mary's stored emails are accessed in violation of the *SCA*, if the computing equipment is managed and supplied by her employer, the court may determine that Mary's employer is a service provider and thus not liable under the Act. [238]

In addition, as Mary's employer has a monitoring policy, some or all of the monitoring activities may fall under the consent exception. The court would need to consider a number of factors, including the detail in the policy itself, its availability, whether Mary signed and acknowledged receipt of the document, and if her employer ensured she fully understood its implications. Additionally, as long as the acquisition of the information is lawful the ECPA does not regulate the uses that may be made of the information, such as for performance review or evidence in disciplinary proceedings.

It is also often difficult to determine with respect to email whether an interception or an access to stored communication has occurred. This can potentially cause problems that make it difficult to take action where a breach occurs.

Another problem is that in order to succeed under either component of the ECPA Mary must demonstrate a subjective and objective reasonable expectation of privacy. Courts in

---

[236] §§ 2511, 2510(12).
[237] § 2701.
[238] *Fraser v. Nationwide Mutual Insurance Co. Inc*, 352 F.3d 107, 115 (3rd Cir. 2003) (Ambro J). See also *Bohach v. The City of Reno*, 932 F. Supp. 1232, 1236 (D.Nev. 1996) (Reed J). CF *Quon v. Arch Wireless Operating Company Inc.*, 2008 U.S. App. LEXIS 12766, *15-24 where the court held the company violated § 2702(a)(1*)* of the *SCA* (which prohibits disclosure of the contents of a communication while in electronic storage) when the Department reviewed transcripts of a police officer's text messages.

the United States are often reluctant to recognise employees have an objective expectation of privacy at work.

Overall, the ECPA is limited in the protection it can afford Mary. It is unlikely given the circumstances that she would be successful in an action under either component of the Act.

Proposed United States Federal Workplace Privacy Legislation

Generally, proposed legislative measures at the national level provide more scope for Mary to raise concerns about the monitoring activities at her workplace. This is particularly so with the *Privacy for Consumers and Workers Act*.

Privacy for Consumers and Workers Act (PCWA)

Mary first needs to consider whether her employer has acted in accordance with the notice requirements, including notification from the Secretary of Labor with respect to her rights under the Act. [239] The notice from her employer should provide Mary with detailed information about the monitoring activities implemented in her workplace. Next, she should examine whether any of the actual monitoring activities violate the Act. Although Mary will not be able to prevent her employer from using monitoring information for performance evaluation, the Act does prohibit this forming the sole basis for such. [240] Mary cannot control the amount of personal information collected by her employer, however she will have an indication (by virtue of the notice requirements) what personal data the monitoring will collect. [241] Mary will also be able to ensure her employer does not disclose data acquired through monitoring to any third party without her prior written consent. [242]

[239] §§ 4(b)(1)-(9), 4(a), S. 984, Privacy for Consumers and Workers Act, 103d Cong., 1st Sess. (1993).
[240] § 8(b).
[241] § 4(b)(2).
[242] § 10(d). A number of exceptions apply including to fellow employees requiring information to perform their duties, and to law enforcement agencies presenting a warrant or similar.

Mary cannot complain over the number of cameras installed by her employer, but will generally be able to prevent her employer using hidden cameras. [243] The Act also prohibits monitoring in bathrooms, locker rooms, and dressing rooms. [244] It is unlikely though that Mary can do anything about the camera in the lunchroom. Although the Act does not regulate the extent and nature of monitoring, as Mary has 5 years or more service, she cannot be subject to periodic or random monitoring. [245] Mary can also request access to and copies of all her personal information collected through monitoring. [246]

The PCWA provides a significant level of protection for employees such as Mary. The notice provisions require reasonably comprehensive details of monitoring activities, and there is some regulation of the use made of the information collected. Mary also has a right of access to personal information held by her employer. Importantly Mary can seek a civil remedy where she suspects a breach. [247]

Notice of Electronic Monitoring Act (NEMA)

The Act imposes a civil penalty on employers who intentionally conduct monitoring in contravention of the notice provisions. [248] Thus, the obligation is on Mary's employer to ensure she receives the requisite notice before any monitoring commences, or where a material change to the monitoring procedure occurs. [249] Mary should also check that the notice contains the required information including the frequency of monitoring, and the type of information to be collected. [250] The notice must be given "…in a manner reasonably calculated to provide actual notice,…." [251] However, it is somewhat unclear as to what constitutes actual notice, and this may provide some difficulty for Mary if a dispute arises. NEMA also requires Mary's employer to provide her with notice on an

[243] § 11(2).
[244] § 10(b)(1)-(3).
[245] § 5(b)(3).
[246] § 7(a).
[247] § 12(c).
[248] § 2711(a)(1), H.R. 4908, Notice of Electronic Monitoring Act, 106th Cong., 2d Sess. (2000).
[249] § 2711(a)(1),(3).
[250] § 2711(b)(1)-(4).
[251] § 2711(b).

annual basis. [252]

As with PCWA, the benefit for Mary in receiving notice is she will have some details of the monitoring practices implemented by her employer. NEMA does not allow Mary to complain about the extent of monitoring, the number, type or deployment of cameras, the use of the information for performance appraisal or similar matters except in so far they relate to the notice requirements. Although there is far less scope for complaint under NEMA than the PCWA, the Act provides some minimal protection for Mary regardless of whether she works in the public or private sector, and also allows her to pursue a civil remedy where a breach occurs. [253]

Employee Changing Room Privacy Act ("ECRPA")

ECRPA prohibits employers engaging in video or audio monitoring in restrooms and similar areas where employees change clothing. [254] The Act does not apply to any other type of monitoring, or video and audio monitoring in other locations of the workplace such as the lunchroom. As such, the legislation does not really address any of Mary's current concerns. The ECRPA is important though in providing employees with some level of privacy in non-production areas of the workplace, and the opportunity to take civil action. [255]

State Law in the United States

There is significant diversity with respect to privacy protection at the state level. For present purposes, I focus on Mary's options under existing workplace privacy legislation in Connecticut, Delaware, California, West Virginia, and Rhode Island, and proposed measures from Georgia, California, Minnesota and Arkansas. I also examine the tort of Intrusion Upon Seclusion. In general, the above measures apply to Mary regardless of

[252] § 2711(a)(2).
[253] § 2711(d).
[254] § 2, H.R. 582, Employee Changing Room Privacy Act, 109th Cong., 1st Sess. (2005).
[255] § 4.

whether she works in the public or private sector.

Existing Workplace Privacy Legislation at the State Level

Provisions regulating electronic monitoring are contained in Connecticut's General Labor Statute. [256] As with NEMA the main obligation on employers is to provide prior written notice of monitoring.

The obligation is on Mary's employer to ensure she receives the requisite notice before monitoring commences. [257] The only required content in the notice is that it details the types of monitoring that will occur. [258] Placing the notice "…in a conspicuous place…" where it "…is readily available for viewing…" by Mary and other employees discharges her employer's obligation with respect to providing actual notice. [259] This requirement is somewhat clearer than is the case with NEMA, and may assist Mary where there is a dispute over the provision of actual notice.

An employer does not need to provide notice where he or she reasonably believes an employee is engaged in unlawful conduct, or conduct that violates the employer's or other employees' legal rights, or creates a hostile work environment, and monitoring may produce evidence of such. [260] Although the Act does not apply to criminal investigations, an employer may use information acquired by monitoring during any such inquiry to discipline an employee. [261]

As the only requirement is to provide notice, the Act offers little scope for Mary to address any of her concerns. Even if there is a breach, Mary cannot pursue a personal remedy. The Act provides for the imposition of a civil penalty following a hearing by the Labor Commissioner. [262] The maximum fine is $500 for the first offence, $1,000 for

[256] *Conn. Gen. Stat*. § 31-48d (2007).
[257] § 31–48d(b)(1).
[258] § 31–48d(b)(1).
[259] § 31–48d(b)(1).
[260] § 31–48d(b)(2).
[261] § 31–48d(d).
[262] § 31–48d(c). The conduct of hearings is in accordance with §§ 4-176e to 4-184.

the second offence and $3,000 for each subsequent offence. [263]

Overall, the legislation provides little comfort to employees who are the subject of intrusions caused by monitoring. There is no regulation of the type or amount of monitoring that may occur and the maximum penalties are relatively low.

Delaware has enacted similar legislation to Connecticut. [264] Before engaging in monitoring Mary's employer has the option of either providing her an electronic notice at least once during any day where she accesses email or the Internet, [265] or a "1-time notice" in written or electronic form. [266] The Act does not prescribe any mandatory information that should appear in the notice. Mary would need to acknowledge in writing or electronically when she has received a "1-time notice" from her employer. [267]

Mary has no recourse to the Act with respect to the cameras, or the use and disclosure of her personal information for performance evaluation or other purposes. As with the Connecticut legislation the only breach relates to failure to provide notice, and the legislation does not regulate any other aspects of monitoring. Penalties under the Act are limited to $100 per violation. [268]

The Act also contains a system management exception that may have implications with respect to Mary's use of email and the Internet. The Act relevantly provides that the provisions "…shall not apply to processes that are designed to manage the type or volume of … electronic mail … or Internet usage, that are not targeted to monitor or intercept the electronic mail … or Internet usage of a particular individual, and that are performed solely for the purpose of computer system maintenance and/or protection." [269] Thus, there is no regulation where the collection of information is incidental to the performance of system maintenance functions.

---

[263] § 31–48d(c).
[264] *Delaware Labor Code*, Title 19, § 705 (2007).
[265] § 705(b)(1).
[266] § 705(b)(2).
[267] § 705(b)(2).
[268] § 705(c).
[269] § 705(e).

The impact of this exception on Mary's ability to protect her personal information will amongst other things, depend on the system configuration and the system management procedures followed. The absence of personal remedies and the minimal fines, combined with the lack of overall regulation means the Act does not provide Mary with sufficient protections against potential intrusions.

California, West Virginia, and Rhode Island have enacted measures similar to Victoria in that they prohibit monitoring in certain non-production areas of the workplace. In California, unless authorised by court order, an employer cannot record by means of audio or video device the activities of an employee in a restroom, locker room, or similar area designated by the employer as a place where employees change clothing. [270] There is also a prohibition on the use of any recordings made in these areas. [271] The Act does not apply to federal government employees. [272] A violation of the Act constitutes an infraction. [273]

The West Virginia Act prohibits the use of electronic surveillance devices to record or monitor employees "…in areas designed for the health or personal comfort of the employees or for safeguarding of their possessions, such as rest rooms, shower rooms, locker rooms, dressing rooms and employee lounges." [274] This prohibition extends to the actions of employer's agents or representatives. [275] Employers breaching the Act are guilty of a misdemeanor and subject to a fine of $500 for the first offence, $1,000 for the second and $2,000 for the third and subsequent offences. [276]

The Rhode Island legislation is similar to that of California. [277] A major difference though is that employees can take civil action and recover damages and reasonable

[270] *Cal Lab Code* § 435(a) (2007).
[271] § 435(b).
[272] § 435(b).
[273] § 435(c). An infraction is a minor offence punishable by a fine <http://www.nolo.com/definition.cfm/Term/1D05D586-169E-4938-89F685445365BC18/alpha/I/>.
[274] *W. Va. Code* § 21-3-20(a) (2007).
[275] § 21-3-20(a).
[276] § 21-3-20(b).
[277] *R.I. Gen. Laws* § 28-6.12-1 (2007).

attorney's fees. [278] It is also possible for Mary to obtain an injunction. [279]

None of these measures provide much assistance to Mary as they only regulate certain types of monitoring in designated areas. As West Virginia prohibits monitoring in "employee lounges", this may mean Mary could complain about the use of the video camera in the lunchroom. If she works in Rhode Island, there is also the possibility of instigating civil action.

Proposed Workplace Privacy Legislation

There have been a number of proposals introduced into state legislatures to regulate monitoring practices. The discussion here focuses on initiatives from Georgia, California, Minnesota, and Arkansas.

The *Privacy for Consumers and Workers Act* sought to amend Title 34 of the Georgia Code. [280] The Bill shares a number of similarities with its federal namesake. I examine some relevant differences that may affect Mary below.

Mary's employer must provide her with simultaneous notice when conducting random or periodic monitoring, or reviewing data acquired in such manner. This notice consists "…of a signal light, beeping tone, verbal notification, or other form of visual or aural notice that indicates electronic monitoring is being conducted." [281] Unlike the federal Bill there is no exemption for Mary from random monitoring because she has 5 years or more service. Although Mary would have a clear indication when her employer is engaging in this type of monitoring, she would still be subject to such monitoring. Mary would also not be able to prohibit her employer from installing hidden video cameras.

In relation to the general notice requirements, Mary's employer is not required to

[278] § 28-6.12-1(c)(1).
[279] § 28-6.12-1(c)(2).
[280] Ga.H.B. 566, Privacy for Consumers and Workers Act, 144th Legis., 1st Sess. (1997-8).
[281] §§ 34-15-3(a)(5), 34-15-3(a)(6)(A)(i). This requirement also appeared in the 1990 version of the Federal PCWA but was part of the general notice requirements.

provide a description of the electronic monitoring, nor details of the exception to providing notice. Also, the Bill does not contain a definition of continuous monitoring (nor indication whether such includes inspection of video monitoring from remote locations).

As with the federal PCWA, Mary's employer can disclose her personal data to the public in the event it contains evidence of illegal conduct by a public official, or directly and seriously affects public health or safety. [282] However, her employer must first provide notice of the proposed disclosure that also informs Mary she has a right to object. [283] If Mary does lodge an objection (within 48 hours of receiving notice) then disclosure of the data can only occur by court order. [284]

Overall, the Bill provides somewhat the same level of protection and prospects with respect to seeking redress as with the federal legislation. It is the most comprehensive of the proposed (and existing) state measures and if enacted would provide employees with significant safeguards.

The Californian Bill requires Mary receive "…clear and conspicuous notice … either electronically or in writing, in a manner reasonably calculated to provide actual notice,…." [285] Mary must receive notice prior to monitoring commencing or where her employer makes a material change. [286] Mary's employer must detail the form of communication or activities subject to monitoring, and the kinds of information obtained, "…including whether activities or communications or computer usage not related to the employer's business are likely to be monitored." [287]

[282] § 34-15-5(b)(2)(A).
[283] § 34-15-5(b)(2)(B)(i).
[284] § 34-15-5(b)(2)(B)(ii).
[285] § 436(c)(1), Cal. Senate Bill 1841 (2003-4).
[286] § 436(b).
[287] § 436(c)(1).

The Bill explicitly states that the placement of signs in the workplace does not discharge her employer's obligations with respect to providing notice. [288] Employers in violation of the Act are guilty of a misdemeanor. [289]

The Bill is similar to some existing laws in that it imposes a notice regime that provides Mary with some indication of the monitoring activities occurring in her workplace. Although Mary would know about any monitoring of non-business usage, the Bill does not provide any protections with respect to the collection of such information. The Bill also does not address her concerns over the installation of cameras, or the use and disclosure of information acquired through monitoring, or its use for performance review or similar matters.

The Bill was subject to various amendments having the effect of weakening protections for employees. For example, this included removing the right of employees to take civil action against employers, and that employers provide notices to employees on an annual basis. [290] Other changes included removing the requirement that employers inform about the means and frequency of monitoring, and how the information will be stored, used, and disclosed. [291]

The Minnesota Bill also requires providing employees with prior written notice before the implementation of monitoring activities. [292] The notice must provide Mary with details concerning the type and frequency of monitoring, the information to be collected, its intended use, and outline the company's policy regarding personal use of company owned equipment. [293] An updated notice is required when there is a change in the type of monitoring. [294] As long as Mary's employer meets the notice requirements, he or she can use the information obtained though monitoring to discipline or discharge her. [295]

[288] § 436(c)(2).
[289] See the Preamble.
[290] Franchise Tax Board, 'Summary Analysis of Amended Bill' - Amended Date 19 April 2004.
[291] Ibid, Amended Date May 24 2004.
[292] § 2(2), Minn.H.F. 3036, Electronic Monitoring of Employees Restricted, 81st Legis., Reg. Sess (1999-2000).
[293] § 2(2).
[294] § 2(2).
[295] § 3.

The focus of the legislation is on monitoring the use of email, Internet, and the telephone. The definition of electronic monitoring reflects this and does not encompass video monitoring. [296] In relation to Mary's other concerns, as with many of the other measures canvassed, there is no avenue for complaint about the extent of personal information collected, or the type, nature and frequency of monitoring activities. Mary can file suit for damages where she is "…injured by the violation…." [297] Mary is also entitled to reasonable attorney's fees where she can demonstrate her employer knowingly or recklessly violated the Act. [298] Mary can also seek injunctive relief. [299] If the court finds a violation has occurred, or grants an injunction, it has the discretion to award any other equitable relief appropriate in the circumstances, including ordering reinstatement and payment of back pay. [300] These aspects render the Bill somewhat more functional than the proposed Californian measure, although it still does not constitute a substantive regulatory framework.

A Bill to requiring employees be provided with notice was introduced in the Arkansas House of Representatives in 2001. [301] Electronic monitoring includes the collection of information by any means other than direct observation. [302]

The Bill combines a notice provision detailing the types of monitoring that can occur, with a prohibition on monitoring in areas "…where an employee has an absolute expectation of privacy such as bathrooms, locker rooms and changing areas." [303] Mary's employer must provide her with access to her records in circumstances where she wishes to dispute any findings based on electronic data. [304]

---

[296] § 1(4).
[297] § (4)(1). Mary would also need to determine what constitutes an "injury" for the purposes of the Act.
[298] § (4)(1).
[299] § (4)(2). A state county or city attorney and a collective bargaining agent also have standing to seek an injunction.
[300] § 4(3).
[301] Ark.H.B. 1291, An Act Requiring Notice to Employees of Electronic Monitoring by Employers; and for Other Purposes, 83rd Gen. Assem., Reg. Sess. (2001).
[302] § 1(1).
[303] § 2(a).
[304] § 2(c).

Personal remedies are not available; instead, breaches are subject to a civil penalty levied through the office of the Director of the Department of Labor. [305] The maximum penalty is $500 for the first offence, rising to $3,000 dollars for the third and subsequent violations. [306] Each day any violation continues constitutes a separate offence. [307]

There is little Mary can do except ensure her employer is meeting the notice requirements. Although there is a prohibition on monitoring in areas where employees have an absolute expectation of privacy, this would not prevent her employer from operating cameras in the lunchroom or similar areas of the workplace.

With the exception of Georgia, the above measures are mainly limited to providing notice and do not adequately regulate monitoring. This leaves employees such as Mary with little protection or scope for redress.

Intrusion Upon Seclusion

As noted in Chapter Two the most relevant privacy tort with respect to electronic monitoring in the workplace is Intrusion Upon Seclusion ("Intrusion"). In order to succeed Mary must show:

1) an intentional intrusion;
2) into the private affairs of another;
3) in a manner which is highly offensive to a reasonable person.

Determining what is "offensive" involves consideration of "…the degree of intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded." [308] Courts often merge the 'highly offensive' and

[305] § 4(a).
[306] § 4(a).
[307] § 4(b).
[308] *Miller v. National Broadcasting Company* (1986) 187 Cal. App. 3d 1463, 1483-4 (Hanson J).

'reasonable expectation of privacy' requirements and consider them together. [309] With respect to the workplace, courts take into consideration the employer's normal business practice, the purpose and methods used to monitor employees, and also attempt to balance the competing interests involved. [310]

The monitoring conducted by Mary's employer would be clearly intentional. The problem arises with meeting the other elements. Unless the monitoring was especially intrusive (for example placing cameras in toilet areas or similar, or where particularly sensitive personal information was collected and misused), it would be difficult for Mary to prove she had either a reasonable expectation of privacy, or that the activity was highly offensive to a reasonable person. The mere presence of cameras (even if not visible), the use of data collected for performance reasons, the incidental collection of her personal information, or being filmed performing her usual work routine is unlikely to be sufficient.

Acosta v. Scott involved the use of a hidden video camera by an employee to film his employer (Scott Borre) in the company offices. [311] Later, a local nightly news program showed the video in relation to a story about employment practices. [312] The Court held the fact Borre worked at the company was not a private matter, and filming him in a shared area of the workplace did not violate his reasonable expectation of privacy. [313] Case law discussed in Chapter Two also demonstrates some of the difficulties that are faced by plaintiffs with respect to demonstrating they possess a reasonable expectation of privacy at work. [314]

---

[309] Jared D. Beeson, 'Cyberprivacy on the Corporate Intranet: Does the Law Allow Private-Sector Employers to Read their Employees' E-mail?' (1998) 20 *Hawaii Law Review* 165, 210 (Citing Prosser and Keeton).

[310] Ibid 210-11 (and references therein).

[311] 377 F. Supp. 2d 647, 649 (N.D. Ill. 2005) (Gettleman J).

[312] Ibid.

[313] Ibid 650-2.

[314] *McLaren v Microsoft Corporation*, 1999 Tex. App. LEXIS 4103; *Smyth v. Pillsbury Co*, 914 F. Supp. 97 (E.D. Pa. 1996); *CF. Restuccia v. Burk Technology*, 1996 Mass. Super. LEXIS 367, *9 (Lopez J) where the court determined there were genuine issues of material fact with respect to whether the plaintiffs had a reasonable expectation of privacy in their emails accessed by their supervisor. The cause of action was under Massachusetts law G.L.c. 214, 1B that relevantly reads " 'a person shall have a right against unreasonable, substantial, or serious interference with his privacy.' "

Mary's employer has also implemented a monitoring policy. If her employer was conducting monitoring for a legitimate business reason, and she voluntarily provided the information through her work and non-work activities, then Mary may not have a reasonable expectation of privacy. The act of providing notice in itself may also undermine the reasonableness of Mary's expectation of privacy. [315]

It is unlikely Mary would be successful in an action for Intrusion. Although the tort offers employees (regardless of sector) an opportunity to seek damages and equitable relief, plaintiffs have been mostly unsuccessful in attempting to persuade courts that they enjoy a reasonable expectation of privacy in the workplace. This would also likely be the case here.

Conclusion

Existing statutory and other measures in both Australian and the United States although offering some scope for complaint, generally provide limited protection of Mary's privacy rights. The majority of the measures involve providing employees notice or prohibit monitoring only in certain prescribed areas. There is also little scope for plaintiff employees to seek personal remedies.

Although important with respect to the privacy of data held by government, information privacy legislation offers little in the way of regulation with respect to monitoring in the workplace. Tort privacy is still in the early stages of development in Australia. However, if the experience in the United States is indicative of what may occur here, then the common law may not provide a viable alternative for Australian employees.
Even where redress is possible, the various measures have differing processes, methods of complaint, and potential financial impact on the plaintiff. Overall, the above analysis provides strong support for the implementation of a national legislative framework to regulate electronic monitoring in the workplace.

[315] *United States v. Bailey*, 272 F. Supp. 2d 822, 835 (D. Neb. 2003) (Piester J).

Chapter Four

A Uniform National Legislative Approach to Regulating Electronic Monitoring in the Workplace

Introduction

This chapter outlines the major themes emerging from the analysis of existing and proposed workplace privacy laws. There is also a brief discussion on the importance of implementing measures to protect employees' privacy, the efficacy of various current approaches, and the benefits of enacting specific workplace privacy legislation.

The main aim of this chapter however, is to propose a uniform national legislative model for regulating electronic monitoring in Australian workplaces. This includes an outline for a draft Bill – the Workplace Surveillance and Monitoring Bill (detailed in Chapter Five).

Key Themes in Workplace Privacy

The foregoing analysis reveals several key themes in workplace privacy. In summary these are:

(a) Employers have the right to implement monitoring in the workplace (regardless of the particular justification). However, employees should not have to relinquish all privacy rights while at work.

(b) Regulation of monitoring practices is necessary to protect the rights of both employers and employees. This is particularly so with respect to preventing the unwarranted disclosure of employees' personal information.

(c) Although using electronic means to monitor employees shares some similarities with traditional methods of supervision, the more invasive nature of the technology

deployed poses a greater threat to employees' privacy.

(d) Existing statutory and other measures in both Australia and the United States have generally failed to adequately protect employees from intrusions caused by electronic monitoring.

(e) Most current approaches are limited in their application to monitoring, operate in isolation, and focus on regulating particular aspects of surveillance activities rather than overall monitoring practices.

(f) Existing and proposed legislation in both Australia and the United States provides a sound framework for the development of a uniform regulatory model.

(g) Enacting uniform legislation provides the most suitable regulatory model for Australian workplaces.

Why Regulation is Necessary

Employees are potentially subject to an increasing array of sophisticated monitoring technologies whilst performing everyday work activities. [1] Though some still believe the use of email and the Internet retains some level of privacy, the technical reality does not support this view. [2]

Issues and concerns over monitoring evidence a common theme, that is, empowered by advances in technology employers are able to collect more detailed and extensive data about employees. [3] Current legislative measures go some way to addressing such

[1] Andrew J. Charlesworth, 'Privacy, Personal Information and Employment' (2003) 1(2) *Surveillance & Society* 217, 218.
[2] Michael Selmi, 'Privacy for the Working Class: Public Work and Private Lives' (2006) 66 *Louisiana Law Review* 1035, 1041-2.
[3] Anthony M. Townsend and James T. Bennett, 'Privacy, Technology, and Conflict: Emerging Issues and Action in Workplace Privacy' (2003) 24(2) *Journal of Labor Research* 195, 196.

concerns, but contain significant deficiencies. [4]

A key difference with information and communication technology systems is that they are both a tool and the medium employees use to interact with co-workers and others, thus "…defining both the nature of the work and the social environment in which it occurs." [5] Because a greater degree of personal as well as business use is possible with such systems, it is important to determine what activities constitute personal use, the extent of personal use permitted, and the level of privacy afforded personal and business use. [6]

Employees and employers have differing expectations with respect to monitoring partly "…because employees are largely unaware of the imperatives for monitoring and usually abysmally ignorant about the prevalence, ease and scope of monitoring." [7] Using technology to gather information about employees is more problematic than traditional forms of supervision as "…employers have the ability to carry out the monitoring secretly, and because monitoring can be continuous and all-encompassing." [8] Also, "…the impact which computer monitoring has on employees' privacy may depend on the type of monitoring that is conducted." [9]

The right to privacy is important because it protects essential values such as autonomy and dignity. [10] For example, monitoring that intentionally acquires the content of personal emails, and logs non-business related website visits inhibits private communications thus affecting "…personal autonomy and the development of ideas, as

---

4 See discussion of Victorian and Commonwealth legislation in Victorian Law Reform Commission, *Workplace Privacy Final Report* (2005), [2.17]-[2.22].

5 Townsend and Bennett, above n 3, 196.

6 Ibid 196-7.

7 Moira Paterson, 'Monitoring of Employee Emails and Other Electronic Communications' (2002) 21(1) *University of Tasmania Law Review* 1, 8.

8 Hazel Oliver, 'Email and Internet Monitoring in the Workplace: Information Privacy and Contracting-Out' (2002) 31(4) *Industrial Law Journal* 321, 327 (Citing Bilsen, Conlon).

9 Lenny Roth, 'Workplace Surveillance - Briefing Paper No. 13/04' New South Wales Parliamentary Library Research Service (2004), 26. For example covert as opposed to overt monitoring, whether it is continuous or infrequent, or whether it involves reading the contents of communications instead of just monitoring the amount of email traffic or web usage.

10 Oliver, above n 8, 323.

well as personal dignity and well-being." [11] Even "…the mere threat of surveillance may be enough to cause concern…" as "…the knowledge that one might be being observed is enough to control behaviour." [12]

Stress, lack of trust, alienation, and lack of self-esteem are other symptoms experienced by employees subject to systematic monitoring and surveillance. [13] Those affected by a diminution in their information privacy are "…more vulnerable to discrimination..." with such loss also having an "…adverse impact on personal autonomy, integrity and dignity, and consequently on our development as individuals, as well as on our relationships with others." [14]

Overall, the lack of control employees are able to exercise over the type and amount of information collected and stored by their employers is a major concern. There is also the issue of legitimacy regarding the manner in which an organization collects and manages personal information, and whether such practices go beyond that deemed acceptable in the circumstances. [15]

The Victorian Law Reform Commission in its Final Report on workplace privacy stated privacy in the workplace requires "…explicit recognition and protection.…" [16] With respect to workplace privacy "…regulation is necessary if we are to provide meaningful protection of privacy in Australia in accordance with our international obligations." [17] The need for reform results from: [18]

> the rapid advances in technology that have occurred and are continuing to occur;
> the difficulties in obtaining meaningful worker consent to any testing and surveillance practices that are used or proposed to be used;
> the current gaps in legislative protection;

[11] Ibid 328.
[12] Ibid (see footnote reference regarding Bentham's Panopticon).
[13] Joseph Migga Kizza, Jackline Ssanyu, 'Workplace Surveillance' in John Weckert (ed.), *Electronic Monitoring in the Workplace: Controversies and Solutions* (2005), 12-3.
[14] Paterson, above n 7, 11.
[15] See Bradley J. Alge, Gary A. Ballinger et al., 'Information Privacy in Organizations; Empowering Creative and Extrarole Performance' (2006) 91(1) *Journal of Applied Psychology* 221, 222-3.
[16] Victorian Law Reform Commission, above n 4, [2.6].
[17] Ibid [2.5]. Although the Commission believes such regulation should be at the state level.
[18] Ibid [2.31].

the lack of mechanisms to balance the interests of workers and employers.

Modern developments in monitoring and surveillance with their unobtrusiveness and subtlety of application have led to comparisons with Bentham's panopticon. [19] Although this may not represent an accurate reflection of how monitoring will evolve in Australian workplaces, the values identified with the right to privacy continue to be challenged through the increased use of electronic monitoring in the workplace.

The Efficacy of Current Measures

Constitutional Protection

There is no guarantee of a right to privacy under the Australian Constitution. Although it is possible to amend the Constitution to add such a right, [20] history indicates few proposals are successful. [21] Justice Kirby speaking extra-judicially noted, the legal difficulties facing the constitutional reformer are not insurmountable, "[b]ut they may be substantial. They were meant to be." [22]

There is some protection for human rights under the Constitution. [23] However, even if a right to privacy was included in the Constitution, this may not sufficiently protect employees. Unless the amendment specifically referred to intrusions in the workplace,

---

19 Jeremy Bentham developed an architectural model for a prison called the "Panopticon." The design allowed the secret monitoring of a large number of inmates by a small number of unseen guards: see David Lyon, 'Facing the future: Seeking ethics for everyday surveillance' (2001) 3 *Ethics and Information Technology* 171, 175; Dorothy J. Glancy, 'Privacy on the Open Road' (2004) 30 *Ohio Northern University Law Review* 295, 327-32.

20 Section 128 of the Australian Constitution requires the passing of an amendment by an absolute majority in both the Senate and House of Representatives, followed by approval in a referendum by a majority of the electors in a majority of states.

21 To date there have been 19 referendums involving 44 proposals with only 8 granted final approval: see Parliament of Australia, 'Parliamentary Handbook of the Commonwealth of Australia' <http://www.aph.gov.au/library/handbook/referendums/index.htm> at 2 October 2007. One of the successful proposals allows electors in the territories to vote in referendums: see C*onstitution Alteration (Referendums) Act 1977.*

22 The Hon. Justice Michael Kirby, 'A Centenary Reflection on the Australian Constitution: The Republic Referendum, 1999' (Speech adapted from the text of the R G Menzies memorial lecture delivered at King's College, London, 4 July 2000) <http://www.hcourt.gov.au/speeches/kirbyj/kirbyj_menzies.htm> at 2 October 2007.

23 For example, see George Williams, *Human Rights under the Australian Constitution* (1999).

the experience in the United States indicates this is unlikely to be of assistance to employees with respect to electronic monitoring. [24]

Privacy Tort

There have been a number of instances in recent times where courts in Australia have recognised a common law right to privacy. As there are few decisions at this point, and so far, none have gone on appeal, it is extremely difficult (and perhaps unwise) to speculate on the development of this tort in Australia. In such circumstances, it is reasonable to look (with caution) at overseas experience. [25]

Intrusion Upon Seclusion is arguably the most relevant tort in the United States with respect to workplace privacy. For the most part plaintiff employees in the United States have not met with much success when pursuing remedies under this cause of action. As the tort of invasion of privacy is only in its infancy in Australia, an assessment of its effectiveness with respect to electronic monitoring awaits further development and refinement by the courts.

Current Privacy Legislation

The Commonwealth *Privacy Act* and state counterparts have some limited application to workplace surveillance and monitoring. The Australian Law Reform Commission ("ALRC") is currently conducting a review into Australia's privacy framework. [26] According to the discussion paper, since the Privacy Act came into force "…advances in information, communication and surveillance technologies have created a range of

[24] There are also those who have argued that the United States Constitution be amended to reflect changes in technology: see Laurence H. Tribe, 'The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier' (Prepared Remarks for the keynote address at the First Conference on Computers, Freedom and Privacy, March 26 1991).

[25] See Des Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339, 388-9.

[26] Australian Law Reform Commission, *Review of Australian Privacy Law*, Discussion Paper No. 72 (2007).

previously unforeseen privacy issues." [27]

The review focuses on the extent the Commonwealth's *Privacy Act* and related State and Territory initiatives protect privacy in Australia. [28] Amongst the key proposals for reform are measures that may affect employees' privacy rights. These include updating the definition of personal information, reducing the number of exemptions, introducing a statutory cause of action for breach of privacy, and ensuring consistency across jurisdictions. [29]

Currently, private sector employers enjoy an exemption from the provisions applying to employee records. The ALRC recommends this exemption no longer apply. [30] The ALRC also believes that to allow maximum coverage and promote consistency, the *Privacy Act*, rather than industrial relations legislation should regulate the privacy aspects of employee records. [31] The ALRC also recommends the small business exemption be removed. [32]

The ALRC believes the *Privacy Act* should remain technologically neutral. [33] However, the ALRC recommends an amendment to the Act allowing the responsible Minister, in consultation with the Commonwealth Privacy Commissioner, to determine privacy and security standards for relevant technologies for incorporation in legislation. [34]

The statutory cause of action applies to invasions of privacy "[w]here there is a reasonable expectation of privacy in all the circumstances, and the act complained of is sufficiently serious to cause substantial offence,…." [35] Circumstances where this cause of action may arise include where "…an individual has been subjected to unauthorised surveillance; an individual's correspondence or private written, oral or electronic

[27] Ibid [1.4].
[28] Ibid [1.18].
[29] Ibid [1.5].
[30] Ibid Proposal 36-1.
[31] Ibid [36.90].
[32] Ibid Proposal 35-1.
[33] Ibid Proposal 7-1.
[34] Ibid Proposal 7-2.
[35] Ibid [1.5].

communication has been interfered with, misused or disclosed; and sensitive facts relating to an individual's private life have been disclosed." [36]

The review also recommends an alteration to the definition of personal information with the effect "…that once information is able to be linked to an individual—and that individual is able to be contacted or targeted—it would become personal information for the purposes of the Privacy Act." [37] In addition, it is proposed that "...the Office of the Privacy Commissioner should consider technologies that can be deployed in a privacy enhancing way by individuals, agencies and organisations." [38]

The above measures if implemented would go some way to increasing the protections available to employees. Promoting consistency across jurisdictions would address some of the problems in those states where privacy controls are in the form of administrative instrument rather than legislation. Of particular interest is the proposed statutory cause of action for a breach of privacy. Also, removing the small business exemption will provide protection to substantial numbers of private sector employees currently not covered by the Act.

Until such changes are in place, it is not possible to determine exactly what impact they will have on workplace privacy. Even if the proposals are accepted, this may not remove the need for separate uniform workplace surveillance legislation. Although the amendments will render the *Privacy Act* a better vehicle for protecting employees, separate workplace legislation offers the benefit of consistency across workplaces, and flexibility in covering a range of technologies. Specifically targeted legislation can also incorporate other important elements such as the type of surveillance technology used, the provision of notice, and the implementation of acceptable use policies that are essential to the effective regulation of monitoring in the workplace.

---

[36] Ibid. See also Karen Curtis, 'Privacy Law Reform *Consistency, Simplicity, Clarity*' (Speech to Melbourne University Law School, Melbourne, 5 March 2008), 13-15.

[37] Ibid [7.50], Proposal 3–5. Thus such things as a telephone number, email or IP address would constitute personal information "…once a sufficient amount of other information accretes around such points of contact."

[38] Ibid Proposal 7-3.

Workplace Privacy and Industrial Relations Legislation

A number of industrial legislative instruments regulate Australian workplaces, though none specifically address privacy concerns in relation to the use of monitoring. In addition, a variety of legal arrangements are found in the workplace including enterprise bargaining agreements, Australian Workplace Agreements, state awards, and common law contracts. Although the *Workplace Relations Act* contains references to privacy, this is limited to ensuring the confidentiality of discussions and documents in the dispute resolution process. [39]

In the United States, the *National Labour Relations Act* contains a prohibition against unfair labour practices. [40] Plaintiff union members successfully argued their employer breached this section of the Act in banning the distribution of emails containing literature and notices from their union. [41]

In *Colgate-Palmolive Company* the Board held that an employer's use of hidden cameras was a mandatory subject of bargaining. [42] Although the company already used surveillance cameras, these cameras were visible and installed for a different purpose than were the hidden ones. [43] In addition, the location of two of the hidden cameras (one in a rest room and another in the fitness centre) "…clearly raise a concern over an individual's privacy and intrudes into employee's personal and private lives, even if it occurs on what is nominally company property." [44] In *National Steel Corporation* the Board found the company breached the Act where it failed to provide details of hidden cameras to the Union and refused to bargain over the use of the cameras. [45]

Although such rulings are encouraging, the concept of an unfair labour practice or requiring bargaining to occur before installing cameras or other devices may not be

[39] See for example ss 702, 707, 712, 715 *Workplace Relations Act* 1996 (Cth).
[40] 29 U.S.C § 158. Also see § 157 with respect to collective bargaining.
[41] *E. I. du Pont de Nemours & Company*, 311 N.L.R.B. 893, 897 (1993).
[42] *Colgate-Palmolive Company*, 323 N.L.R.B. 515, 519-20 (1997).
[43] Ibid 519.
[44] Ibid.
[45] *National Steel Corporation*, 335 N.L.R.B. 747, 747-8 (2001).

sufficient to adequately address all the issues raised by the use of electronic monitoring.

The varying methods of engaging employees also make it difficult to implement any uniform standard of regulation with respect to monitoring activities. In addition, although some overlap exists, workplace privacy is not strictly an industrial matter. The complexities of the issues involved require specifically targeted solutions, which to remain effective, should operate independently of the mainstream industrial relations framework.

Workplace Surveillance Legislation

At the time of writing, only two states, New South Wales [46] and Victoria, [47] have introduced specific workplace surveillance legislation. Although a significant development, for a number of reasons neither statute provides sufficient protection against intrusions caused by electronic monitoring.

With respect to New South Wales, the *Workplace Surveillance Act* has much in common with some of the existing and proposed measures in the United States. Although comprehensive in relation to the technologies regulated (closed circuit television, email, Internet, and GPS), the Act essentially only regulates by way of notice. As such, it fails to provide employees with adequate protection. In addition, remedies are limited to penalties imposed by the State.

Victoria's regulation is less extensive. The *Surveillance Devices (Workplace Privacy) Act* prohibits the use of optical and listening devices in certain areas of the workplace including toilets, wash rooms and change rooms, or publishing a record or report of communications held in such locations. There is no regulation of electronic monitoring in any other areas of the workplace.

[46] *Workplace Surveillance Act 2005* (NSW).
[47] *Surveillance Devices (Workplace Privacy) Act 2006* (Vic).

Both these statutes are state based and face the similar problems, for example the difficulties faced by organizations that conduct business inter-state, and the ability to provide comprehensive regulation of monitoring activities. Although other states may seek to implement similar measures, a national approach would produce a more comprehensive and workable solution.

Why a Legislative Approach is Preferred

The rationale behind adopting a legislative approach is summarised as follows:

There is no privacy guarantee under the Australian Constitution. Although recently there has been some recognition of the existence of a right to privacy at common law, at this point this is limited to a few lower court decisions.

Although constitutional and common law remedies are widely available in the United States, these offer limited protection to employees.

Information privacy legislation is mostly concerned with regulating the record handling procedures of government agencies and is not equipped to deal with many of the issues raised by monitoring in the workplace.

There are a numerous policies and procedures in existence with respect to technology and monitoring practices. These are predominately found in the public sector. While many of these measures provide useful models for conducting electronic monitoring, they lack legislative force and there is uncertainty with respect to their application and enforcement.

Current Australian industrial relations legislation is mostly silent with respect to privacy. Workplace privacy raises distinct and often complex issues that are not easily resolved within the standard industrial framework.

Although New South Wales and Victoria have enacted specific workplace surveillance legislation, these measures (including their United States counterparts) provide limited regulation of monitoring practices and generally do not provide employees with effective redress where a breach occurs.

A legislative approach offers uniformity, flexibility, and a balanced targeted regulatory framework containing comprehensive protections and remedies for employees.

Importantly, such legislation will recognise an employer's right to conduct monitoring in the workplace whilst protecting the privacy rights of employees.

The Workplace Surveillance and Monitoring Bill

The full text of the proposed Bill is contained in Chapter Five. What follows below is a detailed discussion of the main points of the proposed legislation, and analysis of the rationale behind the adoption of the suggested approach.

The Benefits of Uniform Legislation

It is proposed that any future workplace privacy legislation be enacted at the Commonwealth level. There are significant benefits in adopting national uniform legislation to regulate electronic monitoring in Australian workplaces. Specifically targeted legislation will overcome many of the limitations imposed by the other measures canvassed, and provide an opportunity to implement a comprehensive regulatory regime offering benefits to both employees in terms of protection and remedies, and to employers in the form of a clear and concise framework in which to implement monitoring practices.

The problems and issues highlighted by existing and proposed measures from the United States, New South Wales, and Victoria have assisted the development of the draft

legislation. The Bill provides national consistency, thus abrogating many of the problems that arise through differing state based rules and regulations. The legislation covers both private and public sector employees and small business. [48] In addition, the Act would apply regardless of the manner by which an employee is engaged.

An important part of the draft legislation is the inclusion of policies similar to those that currently enjoy widespread use in the public sector. Acceptable use policies provide written guidelines with respect to employer supplied information and communication technology. Giving these policies legislative force will enhance their application and further refinement, and encourage both employers and employees to consider the issues raised by the use of monitoring technology in the workplace.

Advancing technology also poses problems to existing measures. Only a separate legislative instrument is flexible enough to deal with the rapid change that characterises modern technological development.

In addition, the draft Bill is prepared with fundamental legislative principles in mind. [49] This will ensure the legislation establishes a fair and reasonable regulatory framework. The Bill also contains a process of constant review ensuring the proposed Act will keep pace with changing technology. The legislation also seeks to maintain a balance between the respective rights of employers and employees.

Major Influences

Many factors have influenced the development of the draft Bill. The provisions reflect the principles detailed in the themes discussed earlier. Where appropriate, the draft legislation includes what I consider the beneficial aspects of other legislative schemes,

[48] For a discussion of the benefits of federal legislation see S. Elizabeth Wilborn, 'Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace' (1998) 32 *Georgia Law Review* 825, 879-86; Jill Yung, 'Big Brother IS Watching: How Employee Monitoring in 2004 Brought Orwell's 1984 to Life and What the Law Should Do About It' (2005) 36 *Seton Hall Law Review* 163, 211-20.

[49] See s 4 *Legislative Standards Act 1992* (Qld); Chapter 7, Department of Premier and Cabinet, 'The Queensland Legislation Handbook' (2004).

both existing and proposed. In terms of Australia, the *Privacy Act*, *Workplace Surveillance Act 2005* (NSW), the Victorian Law Reform Commission's draft legislation, and Victoria's *Surveillance Devices (Workplace Privacy) Act 2006* were of assistance in developing key parts of the draft Bill.

Reliance is also placed on many existing and proposed legislative measures from the United States, and a number of other sources, including public sector policies and guidelines for the use of information and communication technology. These are particularly relevant with respect to the sections of the Act that address workplace privacy principles, the implementation of acceptable use policies, and data safeguards. [50] Published guides and journals and other sources are referred to where relevant. [51]

Also included are concepts from United States tort law and Fourth Amendment privacy, in particular, those principles expounded in *O'Connor v. Ortega*. [52] Overall, I have attempted to synthesise the important points discussed in the earlier chapters, incorporating or modifying various aspects to produce effective and workable legislation that is not overly prescriptive, and which provides a sound basis for the development of a regulatory framework.

Aims and Objectives

The proposed legislation aims to address the absence of specific measures to control

[50] See for example Queensland Government Chief Information Officer, 'Use of ICT Facilities and Devices (IS38)' <http://www.qgcio.qld.gov.au/02_infostand/is38_print.pdf>; Office of the Public Service Commissioner,'Use of Internet and Electronic Mail Policy and Principles Statement' <http://www.opsc.qld.gov.au/library/docs/resources/policies/internet_and_email_policy.pdf> at 28 February 2008; Yukihiro Terazawa, 'Privacy, Personal E-mail & E-mail Monitoring in the Workplace in Japan' (2003) 4 *Sedona Conference Journal* 141; American Civil Liberties Union, 'Legislative Briefing Kit on Electronic Monitoring' (2003) <http://www.aclu.org/privacy/workplace/1564res 20031022.html> at 14 May 2007.

[51] These include Office of the Privacy Commissioner, 'Guidelines on Workplace E-mail, Web Browsing and Privacy (30/3/2000)' <http://www.privacy.gov.au/internet/email/index.html>; Electronic Frontiers Australia, 'EFA Model Acceptable Use Policy for Employee Use of the Internet' (2000) <http://www. efa.org.au/Publish/aup.html> at 16 March 2007.

[52] 480 U.S. 709 (1987). With respect to codifying the standards expounded in this case see Wilborn, above n 48, 879-82.

electronic monitoring in the workplace. Even though the New South Wales and Victorian initiatives are encouraging, they do not provide sufficient regulation of monitoring activities or adequately protect employees from potential intrusions. Uniform national legislation is the most viable option to address the privacy issues raised by the increased use of sophisticated technologies to monitor employees. The Bill's overall objectives are summarised as follows:

1. Limit the types of electronic monitoring conducted

   The Bill provides for the monitoring of email and Internet usage and in addition, employers may install closed circuit television cameras.

2. Limit the extent of monitoring

   The Bill contains a number of provisions limiting the nature and extent of monitoring activities employers may conduct.

3. Provide adequate safeguards for employees

   Currently employees (including those in New South Wales and Victoria) remain largely unprotected with respect to the amount and type of data collected through monitoring, and how this data is subsequently controlled and managed.

4. Allow for a reasonable level of monitoring

   The Bill formally recognises that employers have a right to install surveillance technologies and implement monitoring programs in the workplace.

5. Provide a range of remedies to employees

   Lack of adequate personal remedies is a feature of many current legislative

schemes. The legislation will provide reasonable levels of compensation to employees where they can successfully demonstrate an unlawful intrusion has occurred.

6. Allow for changing technology

   The Bill provides the flexibility to adapt to changes in current technology or address concerns caused by new and emerging trends.

7. Clearly define rights and responsibilities

   The privacy principles contained in the draft legislation are technologically neutral. The Bill also gives legislative force to acceptable use policies that outline the party's responsibilities when using employer provided information and communication technology.

8. Promote transparency and accountability

   The Bill contains provisions to ensure monitoring practices are transparent.

9. Provide balanced regulation

   The draft legislation seeks to balance the rights of both employees and employers with respect to the implementation and operation of electronic monitoring in the workplace.

Outline of the Main Provisions

Part 1

Part 1 contains preliminary matters including definitions. The Bill authorises video,

email, and Internet monitoring. Although there are numerous technologies deployed in the workplace, email and the Internet are amongst the most common and widely used applications by employees. There has also been a significant increase in the number of CCTV cameras in workplaces, thus regulating CCTV is particularly important. Discussing the difference between video surveillance and the use of GPS in vehicles the Canadian Privacy Commissioner noted, "…information collected by a video camera is far more intimate. When a video camera is pointed at you, you can't even pause to scratch your nose without that information being collected." [53]

Electronic monitoring is widely defined to include all activities involving the acquisition of an employee's information, whether intentional or otherwise. This means the Act covers the inadvertent collection of an employee's non-business related data. Unlike the legislation in New South Wales and Delaware, this definition would encompass such things as the performance of back-ups and other standard system administration functions. Although such activities in themselves may not constitute monitoring, it could involve the collection of an employee's personal information, and therefore should be subject to regulation. Each of the three regulated technologies is defined separately, the common theme being the acquisition of employee related information by electronic means.

A monitoring program comprises the methods and processes used by an employer (or a third party agent of the employer) to conduct electronic monitoring. Information about the employer's monitoring program forms part of the acceptable use policy. An acceptable use policy is an overarching document, or set of documents, containing policies and guidelines relating to the use of employer provided information and communication technology (discussed in more detail in relation to Part 2 of the Bill).

Employee information is similar to that of personal information in the Commonwealth's *Privacy Act* with the addition of data relevant to monitoring, including email and

[53] Jennifer Stoddart, 'Finding the right workplace privacy balance' (Speech delivered at the Ryerson University Workshop on Workplace Privacy, Toronto, Ontario, November 30 2006) <http://www.privcom.gc.ca/speech/2006/sp-d_061130_e.asp> at 21 October 2007.

Internet server logs. This to some extent reflects the proposal from the Australian Law Reform Commission concerning changes to the definition of personal information. Also included is explicit reference to video footage (with or without audio, or whether live or recorded).

Apart from the standard corporate structures employer is also defined to include supervisors, managers or others who control and direct employees with respect to their work. This could alleviate disputes that may arise over actual or apparent authority to implement monitoring practices, where for instance in larger organizations, an employer may be removed from the day to day decision making process. An employee is defined to include both former and prospective workers, people engaged under labour hire contracts, those employees working for subsidiary companies, volunteers, and other persons whose terms of engagement do not involve remuneration.

Workplace is an employee's usual place of employment. Employers may also conduct monitoring where an employee is at another location (including the home) but only where the employee is performing work from that location and is using employer supplied equipment (see Part 2, Authorised Monitoring). Video monitoring of an employee working from home is a breach of the Act (see section 14(g)). An aggrieved party is an employee, their agent, or authorised representative and includes a parent or lawful guardian.

There are also other additional protections for employees. An employee cannot waive their rights under the legislation unless this is in accordance with a settlement offer. Additionally, an employee's rights are cumulative with respect to any existing measures, which may provide more substantial protection than is offered under this legislation.

Part 2

This section of the Bill outlines the workplace privacy principles. There are four principles, covering the party's rights, authorised monitoring, invasion of privacy and

maintaining employee information. These substantive principles are central to the overall legislative scheme, and provide a standard to guide decision-making with respect to the implementation and resolution of complaints regarding electronic monitoring practices.

The first principle (Respective Rights) describes the overriding assumptions with respect to the party's rights and the conduct of monitoring. Paragraph (a) adopts the suggestion that legislation should explicitly state that an employee may have a reasonable expectation of privacy in the workplace. [54] Recognition of an employer's right to implement reasonable levels of monitoring also forms part of this first principle. Paragraph (c) is adapted from *O'Connor v. Ortega* and states that any decision with respect to the appropriateness or otherwise of a monitoring activity must be done on a case by case basis, and attempt to achieve a balance between the respective rights and obligations of the parties.

The second principle (Authorised Monitoring) sets out guidelines covering what constitutes an authorised monitoring activity. The principles cover the location, nature, type, and extent of monitoring and require a link between monitoring and legitimate commercial activities. This means employers must consider alternative means of collecting the required data and to articulate the purpose(s) behind such collection. This requirement allows for a reasonable level of monitoring, and provides a framework whereby an employee can determine whether monitoring activities are appropriate in the circumstances. This also means employers can then exercise their rights to monitor while ensuring such practices are fair and reasonable.

The third principle (Invasion of Privacy) provides guidance on factors to consider when an alleged breach occurs. Paragraphs (c) and (d) are modified from the test applied under the Californian Constitution and the tort of Intrusion Upon Seclusion. The question is whether a serious intrusion has occurred, and whether such conduct is "offensive" rather than "highly offensive" to a reasonable person. This seeks to overcome the difficulties

[54] Wilborn, above n 48, 879-80.

experienced by plaintiff employees in the United States with respect to demonstrating the "offensiveness" of an intrusion, while ensuring only reasonably significant breaches of an employee's privacy constitute a violation of the Act.

The last principle (Maintaining Employee Information) outlines standards with respect to the collection, use, storage, and disclosure of information. These are similar obligations to those found in the Commonwealth *Privacy Act* and state based equivalents.

Part 3

Part 3 of the Bill requires an employer establish an acceptable use policy with respect to employer provided information and communication technology facilities and devices. These policies are widely used within the public sector and by some private sector organizations. Lack of consistency and legislative authority however can lead to some uncertainty with respect to their application and enforcement. The Bill provides formal recognition of these policies and details a non-exhaustive list of factors for inclusion. The requirement for minimum content ensures uniformity and consistency across workplaces, essential if these policies are to be effective in managing monitoring practices.

The Bill also outlines the party's responsibilities under the policy. This is particularly important where there are allegations of misuse. The Bill ensures certainty with respect to the procedures involved in relation to suspected breaches, and requires employers detail the steps involved in resolving such claims.

Part 4

Part 4 outlines the notice requirements. Provision of prior written notice is a common requirement of the legislation analysed. There are separate notice requirements for existing and new employees, and depending on the circumstances, some non-employees

must also receive notice. The information required in the notice is more extensive than under the majority of the legislation consulted.

This extended notice requirement is in accordance with the legislative aim of providing employees with as much relevant information as possible regarding monitoring practices. Even though this may involve providing a significant amount of detail, under the circumstances it probably does not constitute an onerous burden for employers, and the process of collation should assist them to clarify and refine their monitoring programs.

Notice is also required where there is a material change to the monitoring program. This requirement addresses the situation where an employer significantly alters the technology involved, or the scope and nature of the monitoring process itself. Communication of these changes ensures the monitoring program remains transparent, open, and accountable.

Employers are also required to provide notice to some non-employees who gain temporary access to computing facilities. This requirement is minimal and fully discharges the employer's obligations to such persons. Thus, a person who is not an employee, but who is performing work (for a period of 3 months or more for that employer), is made aware their activities are potentially subject to monitoring.

Generally, the Bill provides that notice be given annually and where there is a material change in the monitoring program. Where a material change in the program occurs within 3 months of the date when annual notice would be required, notice of the material change is sufficient to discharge the employer's obligations with respect to the provision of annual notice for that period.

The Bill also requires the notice be on company letterhead and delivered to the employee. Delivery through internal mail (or to a home address) ensures a reasonable level of formality in the notice process. Where this is impractical, employers can provide

substitute notice by email or fax. Employers are also required to post the notice on the company's website if such exists.

Notice is not required where there is suspicion of unlawful conduct, or behaviour that may have a prejudicial effect on the employer's business or the rights of other employees. In such circumstances, an employer must execute a detailed statement describing the conduct and the circumstances under which the monitoring occurred, and place this on the employee's personal record. Where appropriate, law enforcement or similar officials will have access to this statement.

Failure to provide notice where required is a serious breach of the Act making the employer subject to a civil penalty. An employee affected by monitoring may also seek remedies under Part 6. The Bill also stipulates that receipt of a notice by an employee does not constitute a waiver of their right to a reasonable expectation of privacy, or their consent to the monitoring activities detailed in the notice.

Part 5

Part 5 contains additional conditions with respect to the three approved technologies and general monitoring practices. In accordance with the legislative aim to ensure the monitoring process is open and accountable, the Bill provides that cameras must be in fixed locations and clearly visible to employees. Employers are also required to affix notices in areas where video monitoring is occurring. In addition, there is a prohibition on the installation and use of web cameras or cameras with newer technologies such as intelligent video (which have functions that go beyond simple recording, such as the analysis of captured images). Cameras should also not be concentrated on an individual employee's work area.

The Bill encourages a minimalist approach to monitoring. With respect to email, whilst not prohibiting the monitoring of personal email (sent via an employee's service provider using a web browser) it discourages such activity. In addition, where

reasonable, only the message address or label should be the subject of monitoring. Where employers do monitor message content (for example through the use of key word searches or similar), and such monitoring reveals an anomaly, the Bill requires that any machine-generated results from these searches be verified by a human operator before any action is taken against an employee. Most monitoring is conducted automatically, and this protection would operate in circumstances where the output contains errors, or where searches may produce output which when viewed in isolation, may lead to allegations against the sender or recipient of the email, which with further analysis cannot be substantiated.

Similar conditions are outlined for Internet monitoring. The content of an employee's communication should not be monitored unless necessary, for in many instances, the raw data from the monitoring of sites visited, downloads and similar, should provide sufficient information to determine whether misconduct has occurred. Breach of these provisions attracts a civil penalty.

The Bill also prohibits (unless authorised by law) monitoring in areas such as locker rooms, bathrooms, and similar areas. A breach of this provision also results in the imposition of a civil penalty.

The Bill provides that all information concerning an individual employee acquired through monitoring must form part of that employee's personal record. Monitoring data is often stored in a variety of formats and locations, and there is no requirement that the information reside centrally on the file. However, stipulating that the information is part of the employee's permanent record clarifies the situation both from an administrative perspective, and with respect to accessing remedies under the *Privacy Act* (discussed below).

Section 17 outlines the situation with respect to the use of monitoring in public areas (most commonly the installation of cameras for security purposes). However, employers must still abide by the conditions in section 14 (Video Monitoring).

Section 18(1) of the Bill contains restrictions on disclosure of information to third parties without the express written consent of the employee. The Bill provides that where an employer engages an outside agency to perform the monitoring, disclosure to that agency forms an exception to this general requirement. Disclosure to another employee who has a legitimate need for the data, to a law enforcement official, for litigation purposes, to a public official where a major health and safety issue has occurred, or in relation to a complaint, constitute the other exceptions.

Where an employer seeks to disclose information to a third party, and such disclosure does not meet any of the stated exceptions, the employer must provide the employee with written notice detailing the information to be disclosed. The notice must also inform the employee they have 48 hours to lodge an objection with the employer. If the employee lodges a written objection within the stipulated time, a court order is required before disclosure of the employee's personal data can occur. This provision seeks to ensure that as far as practicable, employees should be able to exercise reasonable control over their information during all stages of the monitoring process.

Part 6

Part 6 contains details of the available remedies. In furtherance of the stated objective to offer flexible personal remedies, employees may seek redress through the *Privacy Act* or at common law.

Recognising that cost can be an inhibiting factor, and to avoid duplication of statutory powers and functions, the Bill provides employees with access to the complaint process under the *Privacy Act*. This offers a less formal and more cost effective means to pursue a remedy. The provisions of the Act requiring a person to initially attempt to resolve the issue with the agency concerned do not apply to complaints made under this legislation.

Under section *52* of the *Privacy Act* the Commissioner can make wide ranging determinations to address many of the concerns raised by employees with respect to

monitoring. In order for employees in the private sector (and those in small business) to obtain such access, amendments to the *Privacy Act* are required. Part 7 of the Bill (discussed below) includes the necessary changes.

The majority of the statutes in the United States provide for a civil action. This is in addition to the rights that public sector employees have under the Fourth Amendment. However, actions by employees under either face the problem of establishing that a reasonable expectation of privacy exists in the workplace.

As discussed above, the Bill explicitly recognises employees may have a reasonable expectation of privacy at work. Should an individual plaintiff employee be successful, damages of $50,000 (maximum) per breach (or an aggregate of $250,000), and $1,000,000 per representative claim are available.

The Bill acknowledges that in many instances an injunction may be the most effective remedy, especially if such is to prevent the continued unlawful disclosure of information. There are other orders the court may make, including reinstatement, or payment of lost wages (where an employee has been dismissed or demoted), alterations to the monitoring program, or changes to how the employer manages employee information.

Employees may wish to pursue other options with respect to remedies. For example, many organizations (particularly in the public sector) have implemented comprehensive internal grievance processes. Employees can also pursue remedies under industrial instruments or similar. Alternate dispute resolution is available through the *Privacy Act*, internal grievance processes, or accessed via the relevant provisions in the *Workplace Relations Act*.

The remedies under the Bill are non-exclusive and offer a balance between litigation and less formal methods. Access to the common law provides an employee full scope to pursue a personal remedy without the burden of first establishing an expectation of

privacy exists. These remedies increase the possibility of disputes being resolved, while allowing for adequate compensation where a serious breach of privacy occurs. Recognising that cost may be a prohibitive factor, legal assistance is available to employees for the conduct of any proceedings commenced under section 20.

Part 7

This section sets out civil penalties imposed for the contravention of certain sections of the Bill. These are sub-sections 11.8 (Where Notice is not Required), 11.9 (Failure to Provide Notice), section 13 (Prohibited Areas), section 14 (Video Monitoring), section 15 (Email Monitoring), and section 16 (Internet Monitoring). These are key provisions of the Act, and it is suggested violation of such, although not warranting criminal sanction, is sufficiently serious to attract a pecuniary penalty order. The existence of a penalty emphasizes the significance of these provisions to the overall operation of the Bill whilst providing a financial disincentive with respect to their breach.

The majority of the content of the penalty provisions relies on recommendations from the Commonwealth Government. [55] In particular, that the structure of the provision be in accordance with that outlined in Schedule 2 to the *Commonwealth Authorities and Companies Act 1997*, with associated additional issues from the recommendations. [56] Currently a penalty unit is set at $110. [57] Differing penalties apply to small business operators and larger corporations. [58] Small businesses are those with a turnover of $500,000 per year or less. The penalty for larger corporations is 5 times higher than that for small business. [59]

---

55 Minister for Justice and Customs, 'A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers' (February 2004), 56-63.

56 Ibid 60-2. See also civil enforcement schemes in the *Environment Protection and Biodiversity Conservation Act 1999* (Cth) and *SPAM Act 2003* (Cth).

57 s 4AA(1) *Crimes Act 1914* (Cth).

58 Minister for Justice and Customs, above n 55, 59-60. The report recommends separate penalties depending on whether the contravention is by an individual or a body corporate. The Bill distinguishes between small businesses and larger employers. The Bill also follows the recommendation with respect to the maximum penalty ($5000 or above).

59 Ibid 60.

There is also an ancillary provision allowing a court to make a compensation order where appropriate. Subsection 22.10 provides for a civil double jeopardy protection for employers. The inclusion of such a provision was the subject of a recommendation by the Australian Law Reform Commission. [60]

Subsection 22.2 details the considerations for determining the value of the penalty, the majority of which is adapted from the recommended model. Subparagraphs 22.2(e) and 22.2(f), (the employer's ability to pay, and the effect on the employer's ability to continue in business) are important protections, particularly where a company has limited assets and might cease business if the court imposes a large penalty. [61] The remainder of this section (including those relating to time limits and evidentiary matters) is adapted from the Commonwealth model.

Part 8

Part 8 establishes a committee to monitor developments in monitoring technology. As the technology involved is subject to rapid change, in order for the Act to remain relevant, it is important that it is subject to regular review. The Bill requires the production of a written report on no less than a quarterly basis.

Review of the Act itself is to occur on or before the second anniversary of its assent. Such review will allow legislators the opportunity to address any major issues arising during the initial period of operation. The review process involves consulting and seeking submissions from affected parties. This provision will allow the legislation to adapt to changes in technology and other factors, and ensure it continues to address its aims and objectives.

---

[60] See Australian Law Reform Commission, *Principled Regulation: Federal Civil and Administrative Penalties in Australia*, Report No. 95 (2002) (Recommendation 11-4).

[61] These provisions are from H.R. 582, Employee Changing Room Privacy Act, 109th Cong., 1st Sess. (2005). The other considerations are adapted from Australian Law Reform Commission, *Principled Regulation: Federal Civil and Administrative Penalties in Australia*, Report No. 95 (2002) (Recommendation 29-1).

Part 9

Part 9 contains the required amendments to the *Privacy Act*, including the removal of the employee records and small business exemptions. The amendment also modifies the definition of personal information in accordance with that of 'Employee Information' in the draft Bill. If the recent proposals by the Australian Law Reform Commission are adopted these amendments may not be required.

Conclusion

There are a number of deficiencies in current approaches to regulating electronic monitoring. The main themes emerging from the research and the analysis undertaken has provided the basis for the adoption of a new regulatory framework in the form of a draft Bill (Workplace Surveillance and Monitoring Act).

Outlined in Chapter Five, the Bill seeks to balance the respective rights in the workplace whilst protecting employees' privacy and providing reasonable avenues for redress where a breach occurs. It offers a flexible and comprehensive alternative to existing measures through establishing a uniform legislative model for regulating the use of electronic monitoring in Australian workplaces.

Chapter Five

Workplace Surveillance and Monitoring Act

Introduction

The purpose of this chapter is to outline a framework that illustrates how the key workplace privacy principles may be enshrined in future legislation. As such, the draft Bill is not intended to comprise a detailed statute in its final form incorporating all the relevant aspects of a future regulatory model.

Although it is proposed that such future legislation be enacted by the Commonwealth, in accordance with the aims and objectives outlined in Chapter One, an examination of the particular issues relating to the constitutional validity of privacy legislation under the Australian federal system is outside the scope of this thesis.

Workplace Surveillance and Monitoring Act

A BILL to authorise and regulate the use of electronic surveillance technologies and electronic monitoring in the workplace, to impose civil penalties for certain infringements of the Act, and to provide remedies to employees whose privacy rights are violated through the use of electronic monitoring.

CONTENTS

Part 1 Preliminary

1. Short Title

This Act may be cited as the *Workplace Surveillance and Monitoring Act.*

2. Commencement

This Act commences on the day or days to be fixed by proclamation.

3. Definitions

In this Act –

"acceptable use policy" means a written document(s) outlining policies and guidelines relating to the use of employer provided information and communication technology facilities and devices.

"aggrieved party" means an employee, their agent, or authorised representative and includes a parent or lawful guardian.

"authorised surveillance technology" means video, email, and the Internet.

"civil penalty order" means an order under subsection 22.1.

"civil penalty provision" means a provision declared by this Act to be a civil penalty provision.

"electronic monitoring" means the interception, collection, storage, recording, reading, listening to, viewing, observing, photographing, transmitting, reporting, examination or analysis of data (collected intentionally or otherwise in a workplace) concerning an employee's activities or communications by means other than direct physical observation.

"email monitoring" means the interception, collection, storage, recording, reading, quarantining, examination or analysis of the content, delivery or other identifying information contained in electronic mail messages sent or received by an employee through employer provided information and communication technology facilities and devices.

"employee" means –

(a) a person currently engaged to perform services by an employer; or

(b) a person who has previously been engaged by an employer to perform services; or

(c) a person who has applied for or is being considered for employment by an employer; or

(d) a person engaged under a labour hire contract or similar arrangement by an employer; or

(e) a person engaged by a related corporation owned or operated by an employer; or

(f) a person performing voluntary work, work experience or other non-remunerated services for an employer.

"employee information" has the same meaning as personal information in section 6 of the *Privacy Act 1988* but also includes:

(a) the contents of server logs, reports or other information (including IP addresses and host names) generated by the use of monitoring software or other means which identify and record an email sent or received by an employee, or an employee's Internet usage; and

(b) closed circuit television camera footage, whether silent or otherwise, or whether recorded in any material form.

"employer" means –

(a) any individual, corporation, partnership, unincorporated association, industrial union or similar involved in trade and commerce, who engages employees to perform duties in a workplace; and

(b) the Crown, or an agency of the Crown; and

(c) any person who has the right to control and direct employees with respect to the way an employee performs their duties, the desired outcomes, and the means by which such outcomes are achieved.

"grievance or complaints process" means an internal grievance process implemented by an employer that incorporates explicit processes and procedures to address alleged breaches of this Act.

"information and communication technology facilities and devices" includes computers, workstations, servers, cameras, removable storage media, printers, networks, telephones, Internet, and electronic mail systems.

"Internet monitoring" means to intercept, collect, store, read, record, examine or analyse any aspect of an employee's use of the Internet.

"intercept or interception" means to access, record, capture, or otherwise acquire employee information by electronic means.

"monitoring program" means the methods, process, procedures, programs, and devices used by an employer (or a third party agent of the employer) to implement electronic monitoring in the workplace.

"notice" means written correspondence provided to an employee affected by electronic monitoring.

"penalty unit" has the meaning given by section 4AA of the *Crimes Act 1914*.

"personal email account" means an email account subscribed to by an employee and supplied by a private service provider.

"small business employer" means a business whose annual turnover for the previous financial year is $500,000 or less.

"video monitoring" means to collect, store, record, view, transmit, report, or analyse visual images (including still photographs) of an employee acquired through the use of closed circuit television cameras.

"workplace" means any premises (including areas immediately adjacent to the workplace) owned or under the control of an employer being the usual place of employment for that employee.

"workplace privacy principles" means any of the workplace privacy principles as set out in section 9 of Part 2 of this Act.

4. Act Binds the Crown

This Act binds the Crown in right of the Commonwealth, of each of the States, of the Australian Capital Territory, the Northern Territory, and Norfolk Island.

5. Waiver of Rights

No rights provided under this Act may be waived by contract or otherwise unless such waiver is part of a written settlement agreed to and signed by the parties pending action or complaint under this Act.

6. Employee Rights Cumulative

The rights of employees under this Act are cumulative to and shall not diminish from any rights granted under any Commonwealth or State statute, other law, regulation, agreement, or other legal redress providing greater protection to employees than allowed for under this Act.

7. Interpreting the Workplace Privacy Principles

For the purposes of interpretation of the workplace privacy principles, each shall be treated as if they were a section of this Act.

8. Relationship to Other Laws

This Act does not apply to authorised actions undertaken pursuant to the *Telecommunications (Interception and Access) Act 1979* or any similar law of the Commonwealth or the States and Territories, or to electronic monitoring administered by law enforcement agencies as may otherwise be permitted in criminal investigations under any Commonwealth, State or Territory statute or regulation.

Part 2 Workplace Privacy Principles

9. Privacy Principles

Principle 1 – Respective Rights

(a) An employee may have a reasonable expectation of privacy with respect to information collected by an employer through electronic monitoring.

(b) An employer has the right to implement electronic monitoring in the workplace.

(c) Any determination regarding the appropriateness or otherwise of a monitoring activity used to collect employee information must be considered on a case by case basis and take into account:

(i) the employee's reasonable expectation of privacy; and

(ii) the employer's need for supervision, control, and effective operation of the workplace.

Principle 2 – Authorised Monitoring

Electronic monitoring of employees in the workplace is authorised where:

(a) The monitoring is conducted using an authorised surveillance technology; and

(b) The employee is performing services for the employer, or performing activities that are necessarily incident to the performance of such services, or is acting to protect the employer's rights or property; and

(c) The employee is in the workplace, or if performing work from home or other location, is using employer supplied equipment at that location; and

(d) The monitoring is conducted during the employee's normal working hours; and

(e) Any information collected is for a legitimate business purpose; and

(f) Monitoring is the most effective method of achieving the business purpose; and

(g) Monitoring is conducted by authorised personnel; and

(h) Monitoring is not conducted in an arbitrary or random manner; and

(i) The monitoring method(s) deployed are transparent and appropriate in the circumstances given the nature of the information required; and

(j) The monitoring is not conducted on a continuous basis unless such is necessary to protect health and safety, or is warranted for a legitimate business purpose; and

(k) The sole use of any information collected through monitoring is not for performance evaluation or to discipline, dismiss or otherwise punish an employee; and

(l) The least intrusive method of acquiring information is used; and

(m) Any resulting intrusion is not so severe as to outweigh the necessity for obtaining the information; and

(n) The monitoring is otherwise required or authorised by law.

Principle 3 – Invasion of Privacy

Any determination regarding an alleged violation of an employee's privacy must consider:

(a) The party's rights and obligations; and

(b) Whether the monitoring activity was authorised; and

(c) Whether the intrusive conduct constitutes a serious invasion of privacy; and

(d) Whether the intrusion would be seen as offensive by a reasonable person; and

(e) The nature of the information collected; and

(f) Whether the monitoring subject of the alleged breach was reasonably related in scope to the circumstances that justified monitoring in the first place; and

(g) The number of employees who are subject to the same type and extent of monitoring; and

(h) Whether alternative methods could have been used to obtain the required information.

Principle 4 – Maintaining Employee Information

(a) Information collected through electronic monitoring should be relevant to a business function or requirement of the employer, and the collection process must be necessary for, or directly related to, such function or requirement.

(b) An employee has the right to access all information collected about them through their employer's use of electronic monitoring.

(c) An employee has the right to dispute and request deletion or alteration of inaccurate information held by an employer.

(d) An employer must implement procedures to protect all employee information collected through electronic monitoring from unauthorised access, use, modification, disclosure, or similar misuse.

Part 3 Acceptable Use Policy

10. Acceptable Use Policy Requirements

10.1 Minimum Content

An employer must take reasonable steps to ensure each employee is provided with a copy of the acceptable use policy as soon as practicable after the employee commences work. Such policy must:

(a) Provide details of the employer's monitoring program; and

(b) Provide written guidelines concerning activities that are generally considered to constitute acceptable use of employer provided information and communication technology facilities and devices; and

(c) Clearly indicate whether personal use is permitted and what conditions apply to such use; and

(d) Provide written guidelines concerning activities that are generally considered to constitute misuse of employer provided information and communication technology facilities and devices; and

(e) Detail the consequences where an employee breaches the policy including any disciplinary procedures or penalties that may be imposed; and

(f) Outline a program of appropriate and ongoing training to ensure each employee is aware of and understands their responsibilities under the policy; and

(g) Inform employees of all procedures the employer will use to monitor compliance with the policy; and

(h) Advise employees of the relevant rules concerning the handling of employee information; and

(i) Inform employees of how they can access other relevant policies including the computer security and privacy policies; and

(j) Detail the process whereby employees will be notified of any material changes to the acceptable use policy; and

(k) Refer to relevant Commonwealth legislation including but not limited to the *Privacy Act*, *Archives Act*, *Freedom of Information Act*, and *Crimes Act*.

10.2 Employer Responsibilities

An employer must:

(a) Attempt to resolve any reasonable concerns raised by employees regarding the content of the policy; and

(b) Ensure all policies, practices and systems are consistent with their legal responsibilities under this Act, and

(c) Conduct a detailed investigation into any alleged breaches of the policy including the reporting of suspected unlawful actions to the relevant authorities; and

(d) Ensure disciplinary procedures and penalties imposed on employees who breach the policy are clear, unambiguous, proportionate to the offence and are applied in a manner which is timely, fair and decisive; and

(e) Ensure audit, record keeping, security, confidentiality and quality control policies exist with respect to information collected through monitoring; and

(f) Review the policy as required but no less than on an annual basis.

10.3 Employee Responsibilities

An employee must:

(a) Formally acknowledge all obligations under the policy, and associated documents including the privacy and security policies; and

(b) Not knowingly or intentionally engage in unlawful activities or activities which are in breach of the policy; and

(c) Unless otherwise authorised by the employer, not engage in any personal use of employer provided information and communication technology facilities and devices during designated working hours; and

(d) Immediately delete from their employer's computer system any unsolicited or inappropriate material received from the Internet or by email.

Part 4 Provision of Notice

11. Notice Requirements

11.1 New Employees

An employer must provide a new employee with written notice before they commence work, the content of which must include:

(a) Details of the party's rights and obligations under this Act, and

(b) The forms of communication to be monitored and the surveillance technologies that will be used to collect the information; and

(c) The type of information to be collected including whether an employee's personal email account or other private correspondence will be monitored; and

(d) The duration, frequency and times monitoring will be conducted; and

(e) The location of any cameras; and

(f) How information collected through monitoring will be used, managed, disclosed and disposed of; and

(g) The purpose(s) for monitoring, the benefits, and any potential adverse impacts; and

(h) How printouts, statistics or other reports collected through electronic monitoring are to be interpreted and used; and

(i) The process whereby employees can access information collected about them; and

(j) Any grievance or complaints process the employer has established with respect to resolving disputes involving the use of electronic monitoring.

11.2 Existing Employees

An employer must provide all current employees with notice as described in subsection 11.1 within 30 days from the date of assent of this Act.

11.3 Changes to the Monitoring Program

(a) Where an employer significantly alters the monitoring technology, the scope, and nature of the monitoring process itself, or makes any similar material change to an existing monitoring program, the employer must within 14 days of making such change notify all employees in writing.

(b) Such notice must be substantially in the same form as required under sub-section 11.1.

11.4 Notice to Non-employees

(a) Where a non-employee has temporary access (such access being for a period of not less than 3 months duration) to the employer's information and communication technology facilities and devices, the employer shall provide notice that their activities may be monitored.

(b) Such notice may take any form that is reasonably calculated to inform the individual the subject of the monitoring.

(c) Provision of notice under this subsection fully discharges the employer's obligations to non-employees under this Act.

11.5 Frequency of Notice

(a) An employer shall provide notice meeting the requirements of subsection 11.1 to all employees who will be subject to monitoring on an annual basis.

(b) Should an employer provide notice as required under paragraph 11.3(a), and the provision of such notice occurs within 3 months of the date when the employer would otherwise be required to provide annual notice under paragraph 11.5(a), then such notice shall be deemed to constitute annual notice.

11.6. Form of Notice

(a) The notice should be on company letterhead and either sent directly to the employee though internal mail or posted to their home address.

(b) Where an employer maintains a website, conspicuous posting of the notice on that website.

11.7. Substitute Notice

(a) Where the employer can demonstrate that the cost of providing notice as required by paragraph 11.6(a) is prohibitive due to the size or location of the workforce, or similar circumstances, then the employer may provide employees with substitute notice.

(b) Substitute notice shall be in the form of an email (or facsimile) containing all relevant documentation.

(c) An employer must retain the "read receipt" (or facsimile transfer receipt) concerning any substitute notice sent to an employee and place such on the employee's record.

11.8 Where Notice is not Required

(a) Where the employer reasonably suspects that an employee is engaged in conduct:

(i) that violates criminal law, or

(ii) which may cause the employer's business a real risk of serious damage, or

(iii) will adversely affect other employees' legal rights or interests

and it is reasonable to believe that monitoring will provide evidence of such conduct, then an employer is not required to provide notice to that employee.

(b) Where any of the circumstances described in paragraph 11.8(a) apply, before engaging in electronic monitoring an employer must:

(i) execute a written statement including descriptions of the suspect behaviour, reasons for conducting the monitoring, and where appropriate, identify any specific economic or other loss

or injury to the employer or other employees as a result of the conduct in question; and

(ii) if the suspected conduct is unlawful, notify the appropriate authorities and provide them with a copy of the statement.

(c) A copy of the written statement required by subparagraph 11.8(b)(i) must be placed on the employee's personal record.

(d) Conducting monitoring under this subsection without due cause constitutes a violation of this Act.

Note: This subsection is a civil penalty provision (see section 22).

11.9 Failure to Provide Notice

An employer who conducts electronic monitoring in a workplace without providing notice in accordance with this section contravenes this Act.

Note: This subsection is a civil penalty provision (see section 22).

11.10 Right to Privacy Not Waived

Acceptance of the notice by an employee does constitute a waiver by that employee of their right to a reasonable expectation of privacy, nor indicate consent to any or all of the monitoring activities referred to in the notice.

Part 5 Additional Conditions

12. Electronic Monitoring and Employee Records

All information gathered from electronic monitoring pertaining to an individual employee shall constitute part of that employee's personal employment record.

13. Prohibited Areas

Unless otherwise authorised by law, an employer may not engage in electronic monitoring in bathrooms, change rooms, locker rooms, rest rooms, lunchrooms, sick bays, or similar non-production areas of the workplace.

Note: This subsection is a civil penalty provision (see section 22).

14. Video Monitoring

(a) Cameras must operate from fixed locations and be clearly visible; and

(b) Cameras should not be directed so their sole purpose is to capture images from an employee's individual work area; and

(c) Cameras must not be concealed in other items or otherwise disguised in any manner; and

(d) Cameras which perform functions other than standard recording (such as intelligent video systems) are not permitted to be used for electronic monitoring; and

(e) Web cameras are not permitted to be used for electronic monitoring; and

(f) All areas where video monitoring is occurring must be identified by way of written notice affixed to the wall or other similar structure warning that cameras are installed and operating in that area; and

(g) Video monitoring is prohibited where an employee is performing work related activities from home.

Note: This subsection is a civil penalty provision (see section 22).

15. Email Monitoring

(a) Except in extenuating circumstances an employee's use of a personal email account should not be subject to monitoring; and

(b) The contents of any email message sent or received by an employee should not ordinarily be subject to monitoring; and

(c) Where an employee is suspected of engaging in unauthorised activity, and such suspicion is based upon output automatically generated by the software or machine performing the monitoring, such data must be verified by a person appointed by the employer and a written report produced before any action is taken against the employee.

(d) A copy of any report produced in accordance with paragraph 15(c) above must be placed on the employee's personal record.

Note: This subsection is a civil penalty provision (see section 22).

16. Internet Monitoring

(a) Monitoring other than of the content of any communication transmitted is preferred; and

(b) Where an employee is suspected of engaging in unauthorised activity, and such suspicion is based upon output automatically generated by the software or machine performing the monitoring, such data must be verified by a person appointed by the employer and a written report produced before any action is taken against the employee.

(c) A copy of any report produced in accordance with paragraph (b) above must be placed on the employee's personal record.

Note: This subsection is a civil penalty provision (see section 22).

17. Electronic Monitoring and Public Areas

(a) Electronic monitoring does not include collection of information for security purposes in common areas of the employer's premises held out for use by the public.

(b) Notwithstanding paragraph 17(a), should an employer use cameras for security purposes in a public area, such cameras must be operated in accordance with the requirements of section 14 of this Act.

18. Disclosure of Information

18.1 Restrictions on Disclosure

(a) Employee information collected through monitoring must not to be disclosed to any third party except with the express written consent of the affected employee.

(b) The requirement for written consent is not required in the following circumstances:

(i) where an agent of the employer conducts the monitoring and the disclosure is to the agent's authorised representative; or

(ii) the disclosure is to another employee who requires the information to perform their duties; or

(iii) the disclosure is to a law enforcement agency; or

(iv) the disclosure is pursuant to a request with respect to legal proceedings; or

(v) to a public official or the media in response to a significant public health or safety issue; or

(vi) in furtherance of resolving a complaint to a person who has a legitimate interest in the process; or

(vii) by order of the court.

18.2 Notification of Disclosure

(a) Where an employer seeks to make a disclosure of employee information as provided for under paragraph 18.1(a), and such disclosure does not involve any of the exemptions in paragraph 18.1(b), then the employer must first provide the employee with written notice.

(b) The notice must:

(i) include details of the information subject of the proposed disclosure; and

(ii) inform the employee that they have 48 hours in which to either provide written consent, or indicate their objection to the information being disclosed.

(c) Should an employee (or their agent or lawful guardian) lodge an objection within the stipulated time, the information may only be disclosed after the granting of a court order.

Part 6 Remedies

19. Complaint to the Privacy Commissioner

(a) An aggrieved party may lodge a written complaint with the Commonwealth Privacy Commissioner as provided for under section 36(1) of the *Privacy Act 1988.*

(b) All complaints lodged in this manner will be subject to determination accordance with the procedures and process outlined in Part V of the *Privacy Act 1988*.

(c) Sections 36(1A), 40(1A), and 41(2) of the *Privacy Act* do not apply to complaints lodged under this Act.

20. Civil Action

(a) An employer who causes or allows an invasion of an employee's privacy to occur shall be liable to the employee by such violation for which the employee may seek a civil remedy.

(b) The court may grant:

(i) such preliminary legal, equitable or other declaratory relief as may be appropriate; and

(ii) actual, exemplary and aggravated damages; and

(iii) any other action the court deems appropriate in the circumstances including reinstatement, restoration of benefits, destruction of data, and changes to the monitoring program.

(c) The amount of monetary damages awarded to an employee under subparagraph 20(b)(ii) may not exceed $50,000 per breach or a total aggregate amount of $250,000.

(d) The total aggregate amount of monetary damages awarded against an employer under subparagraph 20(b)(ii) in any representative action may not exceed $1,000,000.

(e) No action may be brought under this subsection unless such action is begun within 3 years from the date of the act complained of, or the date of discovery of the act complained of, whichever is later.

(f) An employee may apply to the Attorney-General with respect to requesting financial assistance in relation to proceedings commenced under this section.

Part 7 Penalties

22. Pecuniary Penalty Order

22.1 Declaration of Penalty

(a) Where a court is satisfied an employer has contravened one of the following provisions it must make a declaration of contravention and the appropriate Minister may seek a pecuniary penalty order:

(i) subsection 11.8 (Where Notice is not Required);
(ii) subsection 11.9 (Failure to Provide Notice);
(iii) sections 13 (Prohibited Areas), 14 (Video Monitoring) 15 (Email Monitoring) and 16 (Internet Monitoring).

(b) Such declaration must detail the Court making the declaration, the penalty provision contravened, the name of the person contravening the provision, and provide details of the conduct that led to the declaration being made.

(c) A declaration of contravention is conclusive evidence of the matters referred to in paragraph 22.1(b).

22.2 Determination of Pecuniary Penalty

In determining the pecuniary penalty, the Court must have regard to all relevant matters, including:

(a) The nature and extent of the contravention and degree of culpability; and

(b) The nature and extent of any loss or damage suffered; and

(c) The circumstances in which the contravention took place; and

(d) Whether any court has previously found the employer in breach of this Act; and

(e) The employer's ability to pay; and

(f) Effect on the employer's ability to continue in business; and

(g) The nature and extent of any co-operation with authorities; and

(h) The level within the organization at which the contravening conduct was authorised.

22.3 Civil Penalty

A court may order an employer to pay the Commonwealth either of the following penalties:

(i) small business employer - a maximum of 50 penalty units for each identified breach; or

(ii) all other employers – a maximum of 250 penalty units for each identified breach.

The above penalties are a civil debt payable to the Commonwealth and are recoverable as a judgment debt.

22.4 Time limit for application

Proceedings for a declaration of contravention, or a pecuniary penalty order, may be started no later than 3 years from the date of the initial contravention, or the date of discovery of the contravention, whichever is later.

22.5 Civil proceedings after criminal proceedings

A court must not make a declaration of contravention or a pecuniary penalty order against an employer for a contravention if the employer has been convicted of an offence constituted by conduct that is substantially the same as the conduct constituting the contravention.

22.6 Criminal proceedings during civil proceedings

(a) Proceedings for a declaration of contravention or pecuniary penalty order against an employer are stayed if criminal proceedings are started or have already been started against the employer for an offence, and the offence is constituted by conduct that is substantially the same as the conduct alleged to constitute the contravention.

(b) The proceedings for the declaration or order may be resumed if the employer is not convicted of the offence. Otherwise, the proceedings for the declaration or order are dismissed.

22.7 Criminal proceedings after civil proceedings

Criminal proceedings may be started against an employer for conduct that is substantially the same as conduct constituting a contravention of a civil penalty provision regardless of whether a declaration of contravention has been made against the employer or any penalty or other award made against that employer.

22.8 Evidence and admissibility in criminal proceedings

(a) Evidence of information given or evidence of production of documents by an employer is not admissible in criminal proceedings

against such employer where the employer has already produced documents or given evidence in proceedings under this Act and the conduct alleged to constitute the offence is substantially the same as the conduct claimed to constitute the contravention.

(b) Paragraph (a) of this sub-section does not apply to a criminal proceeding in respect of the falsity of the evidence given by the employer in the proceedings for the pecuniary penalty order.

22.9 Ancillary Orders

(a) A court may also make an ancillary order directing the payment of compensation to the victim of a contravention of a civil penalty provision.

(b) Such order is in addition to any penalty imposed under subsection 22.3.

(c) In awarding compensation the court must take into consideration any award of damages or action granted the employee under Part 6 of this Act.

22.10 Civil Double Jeopardy

An employer may not be penalised under two or more civil penalty provisions for the same or substantially the same conduct.

Part 8 Miscellaneous

23. Technology Review Committee

(a) The relevant Minister will appoint a committee of appropriately qualified individuals (drawn from both the private and public sector) to review changes to the technology covered by this Act.

(b) The committee shall provide the relevant Minister with a written report detailing any changes and the potential impact such changes may have on the Act’s operation.

(c) Such report is to be provided as and when required, but no less than on a quarterly basis from the date of assent.

24. Review of the Act

(a) The relevant Minister is to review this Act on a date to be determined, such date to be no longer than 2 years from the date of assent.

(b) The review is to examine all aspects of the Act's operation, and provide written recommendations with respect to amendments or any other changes required in order to ensure the Act continues to meet its stated aims and objectives.

(c) The review process must involve a reasonable level of consultation with affected parties, and where appropriate, the inviting of written submissions.

Part 9 Amendment of the Privacy Act 1988

23. Amendments

(a) Section 6(1) - the definition of "personal information" is amended in accordance with section 3 of this Act.

(b) Section 7B(3) (Employee Records Exemption) of the Act is repealed.

(c) Section 6C is amended to add a new subsection as follows:

Workplace Monitoring and Surveillance Act

(6) In this section:

for the purposes of complaints lodged under *Workplace Monitoring and Surveillance Act* reference to 'small business operator' in 6C(1) is removed and sections 6D to 6EA do not apply.

Chapter Six

Conclusion

Although privacy law has a relatively short history, it is becoming an increasingly important area of jurisprudence. Although initially concerned with freedom from unwelcome attention by the press, the concept has expanded to encompass a myriad of unwarranted intrusions into an individual's private life.

Advancements in technology continue to challenge individual privacy rights. This is no less the case in the workplace, which is characterised by a reliance on computer and information technology to perform essential business functions.

Electronic monitoring allows employers to capture significant amounts of information about their employees. Although in both Australia and the United States there are a number of legislative and other measures that achieve some level of protection for employees, none of these sufficiently address all the issues raised by the continued use of electronic means to monitor employees in the workplace.

Effective regulation of monitoring is necessary in order to protect the interests of both employers and employees. Employees have a right to exercise some control over their personal information collected through monitoring, whilst employers need to implement appropriate supervision and control to ensure an efficient and effective workplace. The implementation of a sound legislative regulatory model will allow employers to conduct a reasonable level of monitoring while ensuring employees have a legitimate expectation of privacy whilst at work.

The need for regulation also arises because technology has changed the way we work. In addition, many people are spending increasing amounts of time in the workplace. These factors support the view that workplaces be imbued with some of the privacy protections associated with other locations. This is particularly the case in areas traditionally

considered private, such as rest rooms, change rooms, sick bays, and similar non-production areas.

Some of the proposed changes to the Commonwealth's *Privacy Act* will enhance its applicability to monitoring activities in the workplace. However, this does not remove the need for specifically targeted legislation offering comprehensive strategies to regulate and control the deployment of monitoring technologies.

It is unlikely, at least in the short term, that the development of a common law right to privacy in Australia will provide appropriate protections for employees. Deficiencies in the applicability of information privacy laws, constitutional guarantees, and industrial legislation to workplace intrusions, means that implementing a comprehensive regulatory scheme requires national uniform legislation.

Existing and proposed workplace privacy laws in both Australia and the United States have influenced the proposed draft Bill. The resultant draft legislation incorporates fundamental workplace privacy principles in seeking to produce an effective, flexible, and balanced regulatory model. The legislation allows employers to implement a reasonable level of monitoring, and provides employees with the opportunity to exercise some level of control over information collected in the workplace. The Bill also provides employees with the opportunity to seek effective redress in the event of a breach occurring. Overall, the Bill provides a single point of reference for resolving disputes involving the use of electronic monitoring in Australian workplaces.

Bibliography

Constitutions

Australian Constitution.
Constitution of the State of California.
Constitution of the United States of America.

Legislation

Australia

Commonwealth Authorities and Companies Act 1997 (Cth).
Crimes Act 1914 (Cth).
Crimes (Sentencing Procedure) Act 1999 (NSW).
Industrial Relations Act 1996 (NSW).
Information Act 2002 (NT).
Information Privacy Act 2000 (Vic).
Information Privacy Bill 2007 (WA).
Invasion of Privacy Act 1971 (Qld).
Legislative Standards Act 1992 (Qld).
Liquor Control Reform Act 1998 (Vic).
Monetary Units Act 2004 (Vic).
Ombudsman Act 1978 (Tas).
Personal Information Protection Act 2004 (Tas).
Privacy Act 1988 (Cth).
Privacy Amendment (Private Sector) Act 2000 (Cth).
Privacy and Personal Information Protection Act 1998 (NSW).
Surveillance Cameras (Privacy) Bill 2000 (ACT).
Surveillance Devices Act 1999 (Vic).
Surveillance Devices (Workplace Privacy) Act 2006 (Vic).
Telecommunications (Interception and Access) Act 1979 (Cth).
Workplace Surveillance Act 2005 (NSW).
Workplace Video Surveillance Act 1998 (NSW).

The United States

Ark.H.B. 1291, An Act Requiring Notice to Employees of Electronic Monitoring by Employers; and for Other Purposes, 83rd Gen. Assem., Reg. Sess. (2001).
Cal Lab Code § 435 (2007).
Cal. Senate Bill 1841 (2003-4).
Civil Rights Act of 1871, 17 Stat. 13 (1871).
Conn. Gen. Stat. § 31-48d (2007).
Delaware Labor Code, Title 19, § 705 (2007).
Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).
Ga.H.B. 566, Privacy for Consumers and Workers Act, 144th Legis., 1st Sess. (1997-8).
H.R. 3503, E-Mail Privacy Act of 2005, 109th Cong., 1st Sess. (2005).
H.R. 582, Employee Changing Room Privacy Act, 109th Cong., 1st Sess. (2005).
H.R. 4908, Notice of Electronic Monitoring Act, 106th Cong., 2d Sess. (2000).
Mich. Comp. Laws Ann. § 750.539d (2007).
Minn.H.F. 3036, Electronic Monitoring of Employees Restricted, 81st Legis., Reg. Sess (1999-2000).
National Labor Relations Act, 29 U.S.C §§ 151 – 169 (2006).
Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (1968).
Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974).
R.I. Gen. Laws § 28-6.12-1 (2007).
S. 984, Privacy for Consumers and Workers Act, 103d Cong., 1st Sess. (1993).
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56 115 Stat. 272 (2001).
W. Va. Code § 21-3-20 (2007).

Case Law

AUSTRALIA

Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd (2001) 208 CLR 199.
Australian Municipal, Administrative, Clerical and Services Union v Ansett Australia Ltd [2000] FCA 441.
Church of Scientology Inc v Woodward (1982) 154 CLR 25.
Complaint Determination No.5 of 2004, APrivCmr (19 April 2004).
Complainant L v Tertiary Institution [2004] VPrivCmr6.

Doe v ABC & Ors [2007] VCC 281.
Dragka Mihajlovic and Harlee Pty Ltd tas IGA Waterloo [2007] NSWIRComm 1046.
Giller v Procopets [2004] VSC 113.
Grosse v Purvis (2003) Aust Torts Reports ¶81-706.
Kalaba v Commonwealth of Australia [2004] FCA 763.
Lever v Australian Nuclear Science and Technology Organisation [2007] FCA 1251.
M. Wake v Queensland Rail - PR974391 [2006] AIRC 663 (19 October 2006).
Ng v Department of Education [2005] VCAT 1054.
NW v New South Wales Fire Brigades [2005] NSWADT 73.
Rummery v Federal Privacy Commissioner [2004] AATA 1221.
Seven Network (Operations) Limited v Media Entertainment and Arts Alliance [2004] FCA 637.
Sharma v Sydney South West Area Health Service [2006] NSWIRComm 1157.
Victoria Park Racing and Recreation Grounds Co Ltd v Taylor (1937) 58 CLR 479.

THE UNITED STATES

Acosta v. Scott, 377 F. Supp. 2d 647 (N.D. Ill. 2005).
Adams v. City of Battle Creek, 250 F.3d 980 (6th Cir. 2001).
Alexander v. Federal Bureau of Investigation, 971 F. Supp. 603 (DC. Cir. 1997).
Andersen Consulting v. UOP, 991 F. Supp. 1041 (N.D. Ill. 1998).
Baker v. Department of the Navy, 814 F.2d 1381 (9th Cir. 1987).
Benford v. American Broadcasting Companies, Inc., 554 F. Supp. 145 (D.Md. 1982).
Berger v. New York, 388 U.S. 41 (1967).
Berry v. Funk, 146 F.3d 1003 (D.C. Cir. 1998).
Bohach v. The City of Reno, 932 F. Supp. 1232 (D.Nev. 1996).
Boyd v. United States, 116 U.S. 616 (1886).
Carroll v. United States, 267 U.S. 132 (1925).
Colgate-Palmolive Company, 323 N.L.R.B. 515 (1997).
Doe v. Chao, 540 U.S. 614 (2004).
Dow Chemical Company v. United States, 749 F.2d 307 (6th Cir. 1984).
E. I. du Pont de Nemours & Company, 311 N.L.R.B. 893 (1993).
Fischer v. Mt. Olive Lutheran Church, 207 F. Supp. 2d 914 (W.D. Wis. 2002).
Fraser v. Nationwide Mutual Insurance Co Inc., 352 F.3d 107 (3rd Cir. 2003).
Fred R. McCarroll (DOE/OHA, 1/26/07) Case No. TFA-0186.
Garrity v. John Hancock Mutual Life Insurance Company, 2002 U.S. Dist. LEXIS 8343.
Goldman v. United States, 316 U.S. 129 (1942).

Griggs-Ryan v. Smith, 904 F.2d 112 (1st Cir. 1990).

Griswold v. Connecticut, 381 U.S. 479 (1965).

Hall v. EarthLink Network Inc., 396 F.3d 500 (2d. Cir. 2005).

Haynes v. Office of the Attorney General, 298 F. Supp. 2d 1154 (D. Kan. 2003).

Henke v. United States, 83 F.3d 1453 (DC. Cir. 1996).

Hill v. National Collegiate Athletic Association, 865 P.2d 633 (1994).

In Re Pharmatrak, Inc. Privacy Litigation, 329 F.3d 9 (1st Cir. 2003).

Katz v. United States, 389 U.S. 347 (1967).

Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002).

Kyllo v. United States, 533 U.S. 27 (2001).

Leventhal v. Knapek, 266 F.3d 64 (2nd Cir. 2001).

Lukas v. Triborough Bridge and Tunnel Authority, 1993 U.S. Dist. LEXIS 21065.

Mapp v. Ohio, 367 U.S. 643 (1961).

McCarthy v. De Armit, 99 Pa. 63 (1881).

McLaren v. Microsoft Corporation, 1999 Tex. App. LEXIS 4103.

Miller v. National Broadcasting Company (1986) 187 Cal. App. 3d 1463.

Muick v. Glenayre Electronics, 280 F.3d 741 (7th Cir. 2002).

National Steel Corporation, 335 N.L.R.B. 747 (2001).

Nelson v. Salem State College, 446 Mass. 525 (2006).

New Jersey v. T.L.O, 469 U.S. 325 (1985).

O'Connor v. Ortega, 480 U.S. 709 (1987).

Olmstead v. United States, 277 U.S. 438 (1928).

Quon v. Arch Wireless Operating Company Inc., 2008 U.S. App. LEXIS 12766.

Rakas v. Illinois, 439 U.S. 128 (1978).

Restuccia v. Burk Technology, 1996 Mass. Super. LEXIS 367.

Schmerber v. California, 384 U.S. 757 (1966).

Silverman v. United States, 365 U.S. 505 (1961).

Skinner v. Railway Labor Executives' Association, 489 U.S. 602 (1989).

Smith v. Maryland, 442 U.S. 735 (1979).

Smyth v. Pillsbury Co, 914 F. Supp. 97 (E.D. Pa. 1996).

Steve Jackson Games Inc. v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994).

TBG Insurance Services Corporation v. Zieminski (2002) 96 Cal. App. 4th 443.

Thompson v. Johnson County Community College, 1997 U.S. App. LEXIS 5832.

Thygeson v. U.S. Bancorp, 2004 U.S. Dist. LEXIS 18863.

United States v. Amen, 831 F.2d 373 (2nd Cir. 1987).

United States v. Angevine, 281 F.3d 1130 (10th Cir. 2002).

United States v. Bailey, 272 F. Supp. 2d 822 (D. Neb. 2003).

United States v Barrows, 481 F.3d 1246 (10th Cir. 2007).
United States v. Councilman, 418 F.3d 67 (1st Cir. 2005).
United States v. Knotts, 460 U.S. 276 (1983).
United States v. Leary, 846 F.2d 592 (10th Cir. 1988).
United States v. Maxwell, 45 M.J. 406 (CMA. 1996).
United States v. Mesa-Rincon, 911 F.2d 1433 (10th Cir. 1990).
United States v. Monroe, 52 M.J. 326 (CMA. 2000).
United States v. Simons, 206 F.3d 392 (4th Cir. 2000).
United States v. Slanina, 283 F.3d 670 (5th Cir. 2002).
United States v. Taketa, 923 F.2d 665 (9th Cir. 1991).
United States v. Thorn, 375 F.3d 679 (8th Cir. 2004).
Vega-Rodriguez v. Puerto Rico Telephone Company, 110 F.3d 174 (1st Cir. 1997).
Walker v. Darby, 911 F.2d 1573 (11th Cir. 1990).
Warshak v. United States, 490 F.3d 455 (6th Cir. 2007).
Watkins v. L.M. Berry & Co, 704 F.2d 577 (11th Cir. 1983).
Whalen v. Roe, 429 U.S. 589 (1977).
*Williams v. City of Tulsa***,** 2005 U.S. Dist. LEXIS 37889.

OTHER COUNTRIES

Hosking v Runting [2005] 1 NZLR 1.
Reference Re Public Service Employee Relations Act [1987] 1 S.C.R. 313.

Law Reform Commission Reports

Australian Law Reform Commission, *Principled Regulation: Federal Civil and Administrative Penalties in Australia*, Report No. 95 (2002).
Australian Law Reform Commission, *Review of Australian Privacy Law*, Discussion Paper No. 72 (2007).
Australian Law Reform Commission, *Review of Privacy*, Issues Paper No. 31 (2006).
New South Wales Law Reform Commission, *Invasion of privacy*, Consultation Paper No.1 (2007).
New South Wales Law Reform Commission, *Surveillance Final Report*, Report No. 98 (2005).
Victorian Law Reform Commission, *Workplace Privacy Final Report* (2005).
Victorian Law Reform Commission, *Workplace Privacy Issues Paper* (2002).
Victorian Law Reform Commission, *Workplace Privacy Options Paper* (2004).

Articles

'A Citizen's Guide On Using The Freedom Of Information Act And The Privacy Act of 1974 To Request Government Records' First Report by the Committee on Government Reform and Oversight, March 20, 1997 <http://www.tncrimlaw.com/foia_indx.html>.

Administration Office of the US Courts, *Press Release on Internet Monitoring of Judges & Judiciary Employees* (Aug. 13 2001) <http://w2.eff.org/Privacy/Workplace/Judiciary/20010813_aousc_monitoring_pr.html>.

Alge, Bradley J., 'Effects of Computer Surveillance on Perceptions of Privacy and Procedural Justice' 86(4) *Journal of Applied Psychology* 797.

Alge, Bradley J. and Ballinger, Gary A., et al, 'Information Privacy in Organizations: Empowering Creative and Extrarole Performance' (2006) 91(1) *Journal of Applied Psychology* 221.

Allens Arthur Robinson, 'Overview: Who, what & when: Exemptions' <http://www.aar.com.au/privacy/over/who/exemp.htm?print=true>.

American Civil Liberties Union, 'Legislative Briefing Kit on Electronic Monitoring' (2003) <http://www.aclu.org/privacy/workplace/15646res20031022.html>.

American Management Association, *2005 Electronic Monitoring & Surveillance Survey* <http://www.amanet.org/research/pdfs/EMS_summary05.pdf>.

Anderson, Sandra M., 'Alberta's Statutory Privacy Regime and its Impact on the Workplace' (2006) 43 *Alberta Law Review* 647.

Attorney-General's Department and Department of Employment and Workplace Relations, 'Employee Records Privacy - A discussion paper on information privacy and employee records' (February 2004).

Australian Bureau of Statistics, 'Australian Social Trends 2006, Trends in Hours Worked' (Cat. No. 4102.0).

Australian Privacy Foundation, 'Analysis of the Workplace Surveillance Bill 2005' (16 May 2005) <http://www.privacy.org.au/papers/NSWWPSurvBillAn050516.pdf>.

Ball, Kirstie S., 'Situating workplace surveillance: Ethics and computer based performance monitoring' (2001) 3 *Ethics and Information Technology* 211.

Barron, James H., 'Warren and Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890): Demystifying a Landmark Citation' (1979) 13(4) *Suffolk University Law Review* 875.

Baum, Kevin J., 'E-mail in the Workplace and the Right of Privacy' (1997) 42 *Villanova Law Review* 1011.

Beeson Jared D., 'Cyberprivacy on the Corporate Intranet: Does the Law Allow Private-Sector Employers to Read their Employees' E-mail?' (1998) 20 *Hawaii Law Review* 165.

Bickel, Robert D., Brinkley, Susan and White, Wendy, 'Seeing Past Privacy: Will the Development and Application of CCTV and Other Video Security Technology Compromise an Essential Constitutional Right in a Democracy, or Will the Courts Strike a Proper Balance?' (2003) 33 *Stetson Law Review* 299.

Blakey, Jonathan A., 'Canadian privacy laws: recent milestones' [2004] PLPR 15.

Blinka, Daniel D.,'Overview of Chapter 119. Wire and Electronic Communications Interception and Interception of Oral Communications' (2006) LEXSTAT *18 US NITA PREC 2510.*

Bloustein, Edward J., 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 *New York University Law Review* 962.

Blunn, Anthony S., 'Report of the Review of the Regulation of Access to Communications' (2005) Public Affairs Unit, Australian Government Attorney-General's Department.

Branagan, Mark, 'Eye Spy: Life under the Lens' (2005) 79(11) *Law Institute Journal* 42.

Branch, Philip, 'Lawful Interception of the Internet' (2003) 1(1) *Australian Journal of Emerging Technologies and Society* 38.

Bruemmer, Rene, 'Why Are Cameras Corrosive of Liberties?' (2007) 33(11) *Privacy Journal* 1.

Burrows, John, 'Invasion of privacy – Hosking and Beyond' (2006) 3 *New Zealand Law Review* 389.

Butler, Des, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339.

Bygrave, Lee A., 'Strengthening privacy protection in the Internet environment: A modest program of action' [2006] PLPR 7.

Cabal, Mac, 'California to the Rescue: A Contrasting View of Minimum Statutory Damages in Privacy Torts' (2007) 29 *Whittier Law Review* 273.

Camardella, Matthew J., 'Electronic Monitoring in the Workplace' (2003) 30(3) *Employment Relations Today* 91.

Caragozian, John S. and Warner Jr., Donald E., 'Privacy Rights of Employees Using Workplace Computers in California' Privacy Rights ClearingHouse <http://privacy rights.org/ar/employees-rights.htm>.

Chadwick, Paul 'The Value of Privacy' (Law Week 2006 address at the State Library of Victoria, Melbourne, 23 May 2006).

Chalmers, Robert, 'Orwell or All Well? The Rise of Surveillance Culture' (2005) 30(6) *Alternative Law Journal* 258.

Chapman, Kevin W., 'I Spy Something Read! Employer Monitoring of Personal Employee Webmail Accounts' (2003) 5 *North Carolina Journal of Law and Technology* 121.

Charlesworth, Andrew J., 'Privacy, Personal Information and Employment' (2003) 1(2) *Surveillance & Society* 217.

Clarke, Roger, 'A History of Privacy in Australia' (2002) <http://www.anu.edu.au/people/Roger.Clarke/DV/OzHistory.html>.

Clarke, Roger, 'Have We Learnt To Love Big Brother?' (2005) *Issues 71* 9.

Coles, Clifton,'Fighting Crime with Closed-Circuit Cameras' (2005) *The Futurist* 10.

Corbett, William R.,'The Need For a Revitalized Common Law of the Workplace' (2003) 69 *Brooklyn Law Review* 91.

Cornell University Law School, 'Annotated Constitution: Electronic Surveillance and the Fourth Amendment' (2006) <http://www.law.cornell.edu/anncon/html/index.html>.

Court, Leonard and Warmington, Courtney, 'The Workplace Privacy Myth: Why Electronic Monitoring is Here to Stay' (2004) 29(1) *Oklahoma City University Law Review* 15.

Coyle, Andrea, 'Email and Internet surveillance: do employees have a right to privacy?' (2003) 6(3) *Internet Law Bulletin* 31.

Craver, Charles B., 'Privacy Issues Affecting Employers, Employees, and Labor Organizations' (2006) 66 *Louisiana Law Review* 1057.

Cripps, Alison, 'Workplace Surveillance' (2004), New South Wales Council for Civil Liberties.

Crompton, Malcolm, 'Current Workplace Privacy Issues' (Deacons Speech, 23 October 2003).

Curtis, Karen, 'Good privacy is good business' (Keynote address to New Zealand Privacy Issues Forum, Wellington, 30 March 2006).

Curtis, Karen, 'Privacy Law Reform' (Speech at the Clayton Utz Breakfast Seminar, Canberra, 8 November 2007).

Curtis, Karen, 'Privacy Law Reform *Consistency, Simplicity, Clarity*' (Speech to Melbourne University Law School, Melbourne, 5 March 2008).

David, Ira, 'Privacy Concerns Regarding the Monitoring of Instant Messaging In the Workplace: Is it Big Brother or Just Business?' (2004) 5 *Nevada Law Journal* 319.

Davidson, Alan, 'Under Surveillance' *Proctor* (May 2004) 23.

Department of Premier and Cabinet, 'The Queensland Legislation Handbook' (2004).

DiLuzio, Sarah, 'Workplace E-Mail: It's not as Private as You Might Think' (2000) 25 *Delaware Journal of Corporate Law* 741.

Dirom, Pavlina B., 'Employers' Right To Monitor Employee Email under United States Law' [2001] MurUEJL 26.

Dixon, Nicolee, 'Employees and the Internet – Issues for Public and Private Sector Employers: Research Brief 12/01' (2001) Queensland Parliamentary Library.

Dixon Jr., Robert G., 'The Griswold Penumbra: Constitutional Charter for an Expanded Law of Privacy?' (1965-66) 64 *Michigan Law Review* 197.

Doyle, Carolyn and Bagaric, Mirko, 'The right to privacy and corporations' (2003) 31 *Australian Business Law Review* 237.

Duffy, Dennis P., 'Intentional Infliction of Emotional Distress and Employment at Will: The Case Against "Tortification" of Labor and Employment Law' (1994) 74 *Boston University Law Review* 387.

Ebert, Rebecca, 'Mailer Daemon: Unable to Deliver Message Judicial Confusion in the Domain of E-Mail Monitoring in the Private Workplace' (2002) 1 *Journal of High Technology Law* 63.

Eivazi, Kathy, 'Employees' email privacy and the challenge of advancing technology' [2003] PLPR 46.

Electronic Frontiers Australia, 'EFA Model Acceptable Use Policy for Employee Use of the Internet' (2000) <http:/www.efa.org.au/Publish/aup.html>.

Electronic Frontiers Australia, 'Submission to the Senate Standing Committee on Legal and Constitutional Affairs Inquiry into the Telecommunications (Interception and Access) Amendment Bill 2007' <http://www.efa.org.au/Publish/efasubm-slclc-tiabill2007.html>.

Eltis, Karen, 'The Emerging American Approach to E-Mail Privacy in the Workplace: Its Influence on Developing Caselaw in Canada and Israel: Should Others Follow Suit?' (2003) 24 *Comparative Labor Law and Policy Journal* 487.

Evans, Katrine, 'Show Me the Money: Remedies Under the Privacy Act' [2005] VUWLRev 20.

Evans, Laura, 'Monitoring Technology in the American Workplace: Would Adopting English Privacy Standards Better Balance Employee Privacy and Productivity?' (2007) 95 *California Law Review* 1115.

Fazekas, Christopher Pearson, '1984 is Still Fiction: Electronic Monitoring in the Workplace and U.S. Privacy Law' (2004) *Duke Law and Technology Review* 15.

Finkin, Matthew W., 'Employee Privacy, American Values, and the Law' (1996) 72 *Chicago-Kent Law Review* 221.

Firoz, Nadeem M., Taghi, Ramin and Souckova, Jitka, 'E-Mails in the Workplace: The Electronic Equivalent of "DNA" evidence' (2006) 8(2) *Journal of American Academy of Business* 71.

Fisher, Louis, 'Congress' Role and Responsibility in the Federal Balance of Power: Congress and the Fourth Amendment' (1986) 21 *Georgia Law Review* 107.

Ford, Michael, 'Two Conceptions of Worker Privacy' (2002) 31(2) *Industrial Law Journal* 135.

Ford, Peter, 'Who's Listening? Recording and Monitoring of Personal and Business Communications' (1998) 48(2) *Telecommunication Journal of Australia* 75.

Franchise Tax Board, 'Summary Analysis of Amended Bill' - Amended Date 19 April 2004.

Franchise Tax Board, 'Summary Analysis of Amended Bill' - Amended Date May 24 2004.

Frayer, Charles E., 'Employee Privacy and Internet Monitoring: Balancing Workers' Rights and Dignity with Legitimate Management Interests' (2002) 57(2) *The Business Lawyer* 857.

Freiwald, Susan, 'Online Surveillance: Remembering the Lessons of the Wiretap Act' (2004) 56 *Alabama Law Review* 9.

Fridman, G.H.L., 'A Scandal in Tasmania: The Tort That Never Was' (2003) 22(1) *University of Tasmania Law Review* 84.

Gantt II, Larry O. Natt, 'An affront to human dignity: Electronic mail monitoring in the private sector workplace' (1995) 8 *Harvard Journal of Law and Technology* 345.

Garrow, David J., 'Privacy and the American Constitution' (2001) 68(1) *Social Research* 55.

Geist, Michael, 'Computer and E-mail Workplace Surveillance in Canada: The Shift from Reasonable Expectation of Privacy to Reasonable Surveillance' (2003) 82(2) *Canadian Bar Review* 151.

Gellman, Robert, 'A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board' (2002-3) 54 *Hastings Law Journal* 1183.

Gill, Martin and Spriggs, Angela, 'Assessing the Impact of CCTV' (2005) Home Office Research Study 292.

Glancy, Dorothy J., 'Privacy on the Open Road' (2004) 30 *Ohio Northern University Law Review* 295.

Glancy, Dorothy J., 'The Invention of the Right to Privacy' (1979) 21(1) *Arizona Law Review* 1.

Glancy, Dorothy J., 'United States Privacy Law and the Internet' (2000) 16 *Santa Clara Computer and High Technology Law Journal* 357.

Global Internet Liberty Campaign, 'Privacy and Human Rights: An International Survey of Privacy Laws and Practice' <http://www.gilc.org/privacy/survey/exec-summary.html>.

Gomez-Arostegui, H. Tomas, 'Defining Private Life under the European Convention on Human Rights by Referring to Reasonable Expectations' (2005) 35 *California Western International Law Journal* 153.

Gordon, Philip L., 'Job Insecurity? When it comes to Workplace Surveillance of Electronic Communications, Employers Are Free to Establish the Rules of the Game' (2001-2) 79(4) *Denver University Law Review* 513.

Gormley, Ken, 'One Hundred Years of Privacy' (1992) *Wisconsin Law Review* 1335.

Government of South Australia, 'Annual Report of the Privacy Committee of South Australia - For the year ending 30 June 2007' (September 2007).

Government of South Australia, *Cabinet Administrative Instruction to comply with Information Privacy Principles* (1989, 1992).

Government of South Australia, 'Privacy Committee Members' Handbook Version 1.3' (February 2007).

Gray, Patrick, 'Experts say our privacy is on the verge of becoming extinct', *Sydney Morning Herald* (Sydney), 18 April 2006.

Green, Rachel Sweeney, 'Privacy in the Government Workplace: Employees' Fourth Amendment and Statutory Rights to Privacy' (2004-5) 35(3) *Cumberland Law Review* 639.

Greenberg, Thomas R., 'E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute' (1994) 44 *American University Law Review* 219.

Greenleaf, Graham, 'District Court finds privacy tort: an Australian first' [2003] PLPR 28.

Gross, Hyman, 'The Concept of Privacy' (1967) 42 *New York University Law Review* 34.

Guirguis, Max, 'Electronic Mail Surveillance and the Reasonable Expectation of Privacy' (2003) 8 *Journal of Technology Law and Policy* 135.

Harrison, Bruce S. and Ong, Fiona W., 'E-mail Monitoring and the Attorney-Client Privilege' *LexisNexis Expert Commentaries* (February 2008).

Hartman, Laura P., 'Technology and Ethics: Privacy in the Workplace' (2001) 106(1) *Business and Society Review* 1.

Hartman, Laura P. and Bucci, Gabriella, 'The Economical and Ethical Implications of New Technology on Privacy in the Workplace' (1998) 102-3 *Business and Society Review* 1.

Hill, Gayle, 'Setback for Australian tort of invasion of privacy' (2004) 1(2) *Privacy Law Bulletin* 29.

Hilliard, James W., 'A Familiar Tort That May Not Exist in Illinois: The Unreasonable Intrusion On Another's Seclusion' (1999) 30 *Loyola University Chicago Law Journal* 601.

Holland, Casey, 'Neither Big Brother Nor Dead Brother: The Need for a New Fourth Amendment Standard Applying to Emerging Technologies' (2005-6) 94 *Kentucky Law Journal* 393.

Hong, Haeji, 'Dismantling the Private Enforcement of the Privacy Act of 1974: Doe v. Chao' (2005) 38 *Akron Law Review* 71.

Hornung, Meir S., 'Think Before You Type: A Look at Email Privacy in the Workplace' (2005) 11 *Fordham Journal of Corporate and Financial Law* 115.

Horton, Jonathan, 'The Queensland privacy scheme' [2002] PLPR 5.

Ierodiaconou, Mary-Jane, 'Workplace privacy - the Victorian Law Reform Commission's groundbreaking report' (2005) 2(5) *Privacy Law Bulletin* 65.

Information Commissioner's Office, 'CCTV Code of Practice' (2000).

Information Commissioner's Office, 'Employment Practices Data Protection Code: Part 3 Monitoring at Work' (2003).

'Inslee Introduces Bipartisan Bill to Restore E-Mail Privacy' (29 July 2005) <http://www.house.gov/inslee/issues/privacy/tech_email_privacy.html>.

'Internet privacy survey shows Australian websites lacking – Freehills Internet Privacy Survey Report 2000' [2000] PLPR 1.

Ireland, Oliver and Howell, Rachel, 'The Fear Factor: Privacy, Fear, and the Changing Hegemony of the American People and the Right to Privacy' (2003-4) 29 *North Carolina Journal of International Law and Commercial Regulation* 671.

Jenero, Kenneth A. and Mapes-Riordan, Lynne D., 'Electronic monitoring of employees and the elusive "Right to Privacy" ' (1992) 18(1) *Employee Relations Law Journal* 71.

Jenner, Siobhan, 'The Impact of Computers on Privacy: A Virtual Story' (Speech to the Computer Audit, Control and Security 2005 Conference, Perth, October 2005) <http://www.privacy.gov.au/news/speeches/sp10_05.doc>.

Johnston, Anna and Cheng, Myra, 'Electronic Workplace Surveillance, Part 1: concerns for employees and challenges for privacy advocates' [2003] PLPR 1.

Johnston, Anna and Cheng, Myra, 'Electronic Workplace Surveillance, Part 2: responses to electronic workplace surveillance – resistance and regulation' [2003] PLPR 7.

Josan, Hardeep Kaur and Shah, Sapna K., 'Internet Monitoring of Federal Judges: Striking a Balance Between Independence and Accountability' (2002) 20 *Hofstra Labor and Employment Law Journal* 153.

Kamin, Sam, 'The Private Is Public: The Relevance of Private Actors in Defining the Fourth Amendment' (2004) 46 *Boston College Law Review* 83.

Kende, Mark S., 'The Issues of E-Mail Privacy and Cyberspace Personal Jurisdiction: What Clients Need to Know About Two Practical Constitutional Questions Regarding the Internet' (2002) 63 *Montana Law Review* 301.

Kennedy, Charles H., 'U.S. Court Affirms Employer's Right to Read Employees' Email' (2005) *LexisNexis Martindale-Hubbell Legal Articles*.

Kennedy, Charles H. and Swire, Peter P., 'State Wiretaps and Electronic Surveillance After September 11' (2002-3) 54 *Hastings Law Journal* 971.

Kerr, Orin S., 'Internet Surveillance Law after the USA Patriot Act: The Big Brother that Isn't' (2003) 97 *Northwestern University Law Review* 607.

Kerr, Orin S., 'Searches and Seizures in a Digital World' (2005) 119 *Harvard Law Review* 531.

Kim, Pauline T., 'Privacy Rights, Public Policy, and the Employment Relationship' (1996) 57 *Ohio State Law Journal* 671.

King, David Neil, 'Privacy Issues in the Private-Sector Workplace: Protection from Electronic Surveillance and the Emerging "Privacy Gap" ' (1993-4) 67 *Southern California Law Review* 441.

King, Nancy J., 'Electronic Monitoring to Promote National Security Impacts Workplace Privacy' (2003) 15(3) *Employee Responsibilities and Rights Journal* 127.

Kirby, The Hon. Justice Michael, 'A Centenary Reflection on the Australian Constitution: The Republic Referendum, 1999' (Speech adapted from the text of the R G Menzies memorial lecture delivered at King's College, London, 4 July 2000) <http://www.hcourt.gov.au/speeches/kirbyj/kirbyj_menzies.htm>.

Kirstein, Peter T., 'Early Experiences With the Arpanet and Internet in the United Kingdom' (1999) 21(1) *IEEE Annals of the History of Computing* 38.

LaBancz-Bleasdale, Melisa, 'Employer, Protect Thyself' Messaging News Magazine May/June 2007 Issue <http://www.messagingnews.com/magazine/2007/05/features/employer_protect_thyself.html>.

Landau, Susan, 'What Lessons Are We Teaching?' (2005) 48(6) *Communications of the ACM* 144.

Lasprogata, Gail, King, Nancy J. and Pillay, Sukanya, 'Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada' (2004) *Stanford Technology Law Review* 4.

Lee, Laurie Thomas, 'Watch your E-Mail! Employee E-Mail Monitoring and Privacy Law in the Age of the "Electronic Sweatshop" ' (1994) 28 *John Marshall Law Review* 139.

Lee, Samantha and Kleiner, Brian H., 'Electronic surveillance in the workplace' (2003) 26(2-4) *Management Research News* 72.

Leiner, Barry M., et al, 'The Past and Future History of the Internet' (1997) 40(2) *Communications of the ACM* 102.

Lemons, Bryan R., 'Public Privacy: Warrantless Workplace Searches of Public Employees' (2004) 7 *University of Pennsylvania Journal of Labor and Employment Law* 1.

Levi, Kathryn, 'Guidelines for monitoring workplace emails' (2000) 3(4) *Internet Law Bulletin* 59.

Levin, Avner and Nicholson, Mary Jo, 'Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground' (2005) 2 *University of Ottawa Law and Technology Journal* 357.

Lewis, Ray, 'Employee E-mail Privacy Still Unemployed: What the United States Can Learn from the United Kingdom' (2007) 67 *Louisiana Law Review* 959.

LEXSTAT 10-272 LABOR AND EMPLOYMENT LAW § § 272.0 & 272.02 (2007).

LEXSTAT 1-2 LAW OF THE INTERNET § § 2.03 & 2.11 (2005).

Lindsay, David, 'An exploration of the conceptual basis of privacy and the implications for the future of Australian privacy law' (2005) 29 *Melbourne University Law Review* 131.

Lockton, Vance and Rosenberg, Richard S., 'A Preliminary Exploration of Workplace Privacy Issues in Canada' (2006) Office of the Privacy Commissioner of Canada Contributions Program.

Lyon, David, 'Facing the Future: Seeking ethics for everyday surveillance' (2001) 3 *Ethics and Information Technology* 171.

Lyons, Michael and Le Plastrier, Brett, 'Why Australia needs a tort of invasion of privacy' (2006-7) 89 *Reform* 69.

Manning, Rita C., 'Liberal and communitarian defenses of workplace privacy' (1997) 16(8) *Journal of Business Ethics* 817.

Manning, Stephen, 'Security cameras get eyes, brains', *Sydney Morning Herald*, (Sydney), 12 April 2007.

Marx, Gary T., 'Ethics for the New Surveillance' (1998) 14(3) *The Information Society* 171.

McCallum, Ronald, and Stewart, Andrew, 'The Impact of Electronic Technology on Workplace Disputes in Australia' (2002) 24 *Comparative Labor Law and Policy Journal* 19.

McCartney, Donald R., 'Electronic Surveillance and the Resulting Loss of Privacy in the Workplace' (1994) 62 *University of Missouri-Kansas City Law Review* 859.

McEvoy, Sharlene A., 'E-mail and Internet monitoring and the workplace: do employees have a right to privacy?' (2002) 24(2) *Communications and the Law* 69.

McKay, Robert B., 'The Right of Privacy: Emanations and Intimations' (1965-6) 64 *Michigan Law Review* 259.

McKenzie, Robin, 'The Privacy Act, employee records and email monitoring' (PowerPoint Slides - Office of the Privacy Commissioner Presentation to a workshop hosted by Clearswift Corporation, Perth, 5 March 2003).

McIntosh, Dan, 'e-monitoring@workplace.com: The Future of Communication Privacy in the Minnesota Private-Sector Workplace' (2000) 23 *Hamline Law Review* 539.

McRobert, Andrew, 'Breach of Confidence: Revisiting the Protection of Surreptitiously Obtained Information' (2002) 13 *Australian Intellectual Property Journal* 69.

Meyers, Neville, 'If Big Brother comes to a venue near you! Employee-surveillance issues and the communication professional' (2003) 30(2) *Australian Journal of Communication* 101.

Miller, Seumas, and Weckert, John, 'Privacy, the workplace and the Internet' (2000) 28(3) *Journal of Business Ethics* 255.

Minister for Justice and Customs, 'A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers' (February 2004).

Mishra, Jitendra M. and Crampton, Suzanne M., 'Employee monitoring: Privacy in the workplace?' (1998) 63(3) *S.A.M. Advanced Management Journal* 4.

Mitrou, Lilian and Karyda, Maria, 'Employees' privacy vs. employers' security: Can they be balanced?' (2006) 23 *Telematics and Informatics* 164.

Morris Jr., Frank C., 'The Electronic Platform: Email and Other Privacy Issues in the Workplace' (2003) 20(8) *The Computer and Internet Lawyer* 1.

National Alternative Dispute Resolution Advisory Council, 'Legislating for Alternative Dispute Resolution: A guide for government policy-makers and legal drafters' (2006).

Nehf, James P., 'Incomparability and the Passive Virtues of Ad Hoc Privacy Policy' (2005) 76 *University of Colorado Law Review* 1.

Nijhawan, David Raj, 'The Emperor Has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation in the United States' (2003) 56 *Vanderbilt Law Review* 939.

Nolan, Jim, 'Employee privacy in the electronic workplace Pt 1: surveillance, records and emails' [2000] PLPR 51.

Nord, G. Daryl, McCubbins, Tipton F. and Nord, Jeretta Horn, 'E-Monitoring in the Workplace: Privacy, Legislation, and Surveillance Software' (2006) 49(8) *Communications of the ACM* 73.

Office for the Commissioner for Public Employment, 'Determination 2: Recruitment and Employment of Non Executive Employees' (14 September 2001).

Office for the Commissioner for Public Employment, 'Grievance Resolution: An Information Paper for Managers and Human Resource Practitioners' (March 1997).

Office of Parliamentary Counsel, 'Drafting Directions' (2006).

Office of Parliamentary Counsel, 'OPC Drafting Manual Edition 1.1' (2006).

Office of the Privacy Commissioner, 'Guidelines on Workplace E-mail, Web Browsing and Privacy (30/3/2000)' <http://www.privacy.gov.au/internet/email/index.html>.

Office of the Privacy Commissioner, 'Information Sheet 12: 2001 Coverage of and Exemptions from the Private Sector Provisions.'

Office of the Privacy Commissioner, 'Privacy & Related Legislation in Australia' (2007) <http://www.privacy.gov.au/privacy_rights/laws/index.html>.

Office of the Privacy Commissioner, 'Submission to the Attorney-General's Department and Department of Employment and Workplace Relations Review of Employee Records Exemption' (April 2004).

Office of the Privacy Commissioner, 'The Operation of the Privacy Act Annual Report 1 July 2006-30 June 2007' (2007).

Office of the Public Service Commissioner, 'Use of Internet and Electronic Mail Policy and Principles Statement' <http://www.opsc.qld.gov.au/library/docs/resources policies/internet_and_email_policy.pdf>.

Office of the Victorian Privacy Commissioner, 'Info Sheet 07.02 - A Brief History of Information Privacy' (19 June 2002).

O'Gorman, Daniel P., 'Looking out for Your Employees: Employers' Surreptitious Physical Surveillance of Employees and the Tort of Invasion of Privacy' (2006) 85 *Nebraska Law Review* 212.

Oliver, Hazel, 'Email and Internet Monitoring in the Workplace: Information Privacy and Contracting-Out' (2002) 31(4) *Industrial Law Journal* 321.

Otis, James, 'Against Writs of Assistance' (Notes and Speech delivered before the Massachusetts Superior Court February 24, 1761) <http://www.constitution.org/bor/otis_aganst_writs.htm>.

Otlowski, Margaret, 'Employment Sector By-Passed by the Privacy Amendments' (2001) 14 *Australian Journal of Labour Law* 169.

Oyama, Katherine A., 'E-Mail Privacy after United States v. Councilman: Legislative Options for Amending ECPA' (2006) 21 *Berkeley Technology Law Journal* 499.

Oz, Effy, Glass, Richard and Behling, Robert, 'Electronic workplace monitoring: what employees think' (1999) 27 *Omega International Journal of Management Science* 167.

Parliament of Australia - Department of Parliamentary Services, 'Do Australians have a legal right to privacy?' Research Note No. 37 (14 March 2005).

Parliament of Australia, 'Parliamentary Handbook of the Commonwealth of Australia' <http://www.aph.gov.au/library/handbook/referendums/index.htm>.

Parliament of Australia – Senate Legal and Constitutional References Committee, 'The real Big Brother: Inquiry into the Privacy Act 1988' (2005).

Parliament of Australia – Senate Standing Committee on Legal and Constitutional Affairs, 'Telecommunications (Interception and Access) Amendment Bill 2007 [Provisions]' (August 2007).

Paterson, Moira, 'Monitoring of Employee Emails and Other Electronic Communications' (2002) 21(1) *University of Tasmania Law Review* 1.

Penning, Steven and Magner, Aaron, 'Workplace surveillance and privacy' (2006) *Commercial Law Quarterly* 24.

Persson, Anders J. and Hansson, Sven Ove, 'Privacy at work ethical criteria' (2003) 42(1) *Journal of Business Ethics* 59.

Pivec, Mary E. and Brinkerhoff, Susan, 'E-Mail in the Workplace: Limitations on Privacy' (1999) 26(1) *Human Rights* 22.

Porter II, William G, and Griffaton, Michael C., 'Between the Devil and the Deep Blue Sea: Monitoring the Electronic Workplace' (2003) 70(1) *Defense Counsel Journal* 65.

Posner, Richard A., 'The Right of Privacy' (1977-8) 12(3) *Georgia Law Review* 393.

Posner, Steven C, 'Practice Commentary - Privacy and the USA Patriot Act' (2005) *LexisNexis Martindale-Hubbell Legal Articles*.

President and Fellows of Harvard College, 'A Thinly Veiled Request for Congressional Action on E-Mail Privacy: United States v. Councilman' (2005) 19 *Harvard Journal of Law and Technology* 211.

Privacy Committee of South Australia, 'Privacy Committee Members Handbook Ver. 1.3' (February 2007).

Privacy New South Wales, 'Submission to the Australian Government Discussion Paper on Information Privacy and Employee Records' (29 April 2004).

Prosser, William L., 'Privacy' (1960) 48(3) *California Law Review* 383.

Queensland Government Chief Information Officer, Information Standard 42 (IS42) <http://www.qgcio.qld.gov.au/02_infostand/standards/is42.pdf>.

Queensland Government Chief Information Officer, 'Use of ICT Facilities and Devices (IS38)' <http://www.qgcio.qld.gov.au/02_infostand/is38_print.pdf>.

Reidenberg, Joel R., 'Privacy Wrongs in Search of Remedies' (2002-03) 54 *Hastings Law Journal* 877.

Richardson, Megan, 'Whither breach of confidence: A right of privacy for Australia?' (2002) 26(2) *Melbourne University Law Review* 381.

Roth, Lenny, 'Workplace Surveillance - Briefing Paper No. 13/04' New South Wales Parliamentary Library Research Service (2004).

Roth, Paul, 'Remedies under New Zealand privacy law – Part 1' [2004] PLPR 4.

Roth, Paul, 'Remedies under New Zealand law – Part 3' [2004] PLPR 16.

Rothstein, Lawrence E., 'Privacy or Dignity?: Electronic Monitoring in the Workplace' (2000) 19 *New York Law Journal of International and Comparative Law* 379.

Roundy, Michael D., 'The Wiretap Act- Reconcilable Differences: A Framework for Determining the "Interception" of Electronic Communications Following United States v. Councilman's Rejection of the Storage/Transit Dichotomy' (2006) 28 *Western New England Law Review* 403.

Rustad, Michael L. and Paulsson, Sandra R., 'Monitoring Employee E-mail and Internet Usage: Avoiding the Omniscient Electronic Sweatshop: Insights from Europe' (2005) 7 *University of Pennsylvania Journal of Labor and Employment Law* 829.

SaratChandran, Priya, 'Workplace Privacy and CSR' (2005-6) 87 *Reform* 49.

Schatz, Andrew, 'Online privacy, spam and the Stored Communications Act' Australian Government Solicitor, Commercial Notes No. 13 (8 February 2005).

Schatz, Andrew, 'Recent developments in telecommunications interception and access law' Australian Government Solicitor, Commercial Notes No. 20 (19 September 2006).

Schatz, Andrew and Hill, Graeme, 'The extended reach of the Workplace Surveillance Act' Australian Government Solicitor, Commercial Notes No. 17 (5 October 2005).

Schulman, Andrew, 'Computer and internet surveillance in the workplace' [2001] PLPR 31.

Selmi, Michael, 'Privacy for the Working Class: Public Work and Private Lives' (2006) 66 *Louisiana Law Review* 1035.

Sempill, Julian, 'Under the Lens: Electronic Workplace Surveillance' (2001) 14 *Australian Journal of Labor Law* 1.

Shinder, Debra, '10 ways to monitor company computers' (2006) *TechRepublic* <http://www.zdnet.com au/jobs/resources/soa/10-ways-to-monitor-company-computers/0,130056675,139236448,00.htm>.

Silverman, Craig, 'Smile, Big Brother's watching', *The Globe and Mail*, (Toronto), 24 March 2008.

Sneddon, Mark and Troiano, Riccardo, 'New tort of invasion of privacy and the Internet' (2003) 6(6) *Internet Law Bulletin* 61.

Sonenshein, David A., 'Rule 56. Summary Judgment' (2008) LEXSTAT *US NITA FED RULES CIV PROC R 56.*

Spencer, Shaun B., 'Reasonable Expectations and the Erosion of Privacy' (2002) 39 *San Diego Law Review* 843.

Sproule, Clare M., 'The Effect of the USA Patriot Act on Workplace Privacy' (2002) 43(5) *Cornell Hotel and Restaurant Administration Quarterly* 65.

Stewart, Daniel, 'Protecting Privacy, Property, and Possums: Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd' (2002) 30 *Federal Law Review* 177.

Stoddart, Jennifer, 'Finding the right workplace privacy balance' (Speech delivered at the Ryerson University Workshop on Workplace Privacy, Toronto, Ontario, November 30 2006) <http://www.privcom.gc.ca/speech/2006/sp-d_061130_e.asp>.

Stokes, Pamela P. and Polansky, Sharon, 'It's None of Your Business - Or Is It?' (2001) 17(1) *The Journal of Applied Business Research* 29.

Sullivan, Julianne M., 'Will the Privacy Act of 1974 Still Hold up in 2004? How Advancing Technology has Created a Need for Change in the "System of Records" Analysis' (2002-3) 39 *California West Law Review* 395.

Surveillance Studies Network, 'A Report on the Surveillance Society - For the Information Commissioner' (September 2006).

Swire, Peter P., 'Katz is Dead. Long Live Katz' (2004) 102(5) *Michigan Law Review* 904.

Telford, Paul, 'Gross v Purvis: its place in the common law of privacy' [2003] PLPR 36.

Terazawa, Yukihiro, 'Privacy, Personal E-mail & E-mail Monitoring in the Workplace in Japan' (2003) 4 *Sedona Conference Journal* 141.

The American Law Institute, *Restatement (Second) of Torts* (1977).

Thomas, Trevor, 'The Telecommunications (Interception) Act and the Privacy of Stored Communications' (2005) 55(1) *Telecommunications Journal of Australia* 64.

'Tips on Keeping Workplace Surveillance from Going Too Far' (2006) 83(1) *HR Focus* 10.

Townsend, Anthony M. and Bennett, James T., 'Privacy, Technology, and Conflict: Emerging Issues and Action in Workplace Privacy' (2003) 24(2) *Journal of Labor Research* 195.

Tribe, Laurence H., 'The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier' (Prepared Remarks for the keynote address at the First Conference on Computers, Freedom and Privacy, March 26 1991).

Tutaj, Adam J.**, '**Intrusion Upon Seclusion: Bringing an "Otherwise" Valid Cause of Action into the 21st Century' (1999) 82 *Marquette Law Review* 665.

United States Department of Justice, 'Overview of the Privacy Act of 1974, May 2004 Edition' <http://www.usdoj.gov/oip/04_7_1.html>.

United States Government Printing Office, 'Amendment 4 – Search and Seizure' <http://www.gpoaccess..gov/constitution/pdf2002/022.pdf>.

Warren, Samuel D. and Brandeis, Louis D., 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.

Wasserstrom, Silas J. and Seidman, Louis Michael, 'The Fourth Amendment as Constitutional Theory' (1988) 77 *Georgetown Law Journal* 19.

Watson, Nathan, 'The Private Workplace and the Proposed "Notice of Electronic Monitoring Act": Is "Notice" Enough?' (2001) 54 *Federal Communications Law Journal* 79.

Watson, Penelope, 'Privacy and Law Reform' (2007) 78 *Precedent* 5.

Weeks, Carly, **'**No escaping Big Brother's watchful eyes and ears: Privacy experts warn of a future in which everything we do can be recorded and stored', *The Edmonton Journal* (Edmonton), September 28, 2007.

Wen, H. Joseph, and Gershuny, Pamela, 'Computer-based monitoring in the American workplace: Surveillance technologies and legal challenges' (2005) 24 *Human Systems Management* 165.

Wheelwright, Karen, 'Monitoring employees' email and internet use at work: balancing the interests of employers and employees' (2002) 13 (1) *Journal of Law and Information Science* 70.

White, Jarrod J., 'EMAIL@WORK.COM: Employer Monitoring of Employee E-mail' (1997) 48 *Alabama Law Review* 1079.

Wilborn, S. Elizabeth, 'Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace' (1998) 32 *Georgia Law Review* 825.

Willborn, Steven L., 'Consenting Employees: Workplace Privacy and the Role of Consent' (2006) 66 *Louisiana Law Review* 975.

Wilson, Tony, 'Privacy by degrees' (2004) 1(5) *Privacy Law Bulletin* 78.

Witzleb, Normann, 'Federal Court strengthens privacy enforcement: Seven Network (Operations) Limited v Media Entertainment and Arts Alliance [2004] FCA 637' (2005) 33 *Australian Business Law Review* 45.

Yung, Jill, 'Big Brother IS Watching: How Employee Monitoring in 2004 Brought Orwell's 1984 to Life and What the Law Should Do About It' (2005) 36 *Seton Hall Law Review* 163.

Books

Colucci, Michele, *The Impact of the Internet and New Technologies on the Workplace: A Legal Analysis from a Comparative Point of View* (2002).

Douglas-Stewart, Jeremy (ed.), *Workplace Surveillance Act 2005 (NSW): Handbook and Compliance Guide*: *the essential handbook for complying with workplace surveillance laws in NSW* (2005).

Doyle, Carolyn, Bagaric, Mirko, *Privacy Law in Australia* (2005).

Solove, Daniel J., Rotenberg, Marc and Schwartz, Paul M., *Information Privacy Law* (2006).

Weckert, John (ed.), *Electronic Monitoring in the Workplace: Controversies and Solutions* (2005).

Williams, George, *Human Rights under the Australian Constitution* (1999).

Theses

Clarke, Roger Anthony, *Data Surveillance: Theory, Practice & Policy* (D Phil Thesis, ANU, 1997).

Uteck, E. Anne, *Electronic Surveillance and Workplace Privacy* (LLM Thesis, Dalhouise University, 2004).

Workplace Privacy Web Sites

Australian Privacy Foundation, Workplace Surveillance Page <http://www.privacy.org.au/Campaigns/Workplace/>.

Electronic Frontiers Australia –Workplace Surveillance Resource Site <http://www.efa.org.au/Issues/Privacy/workplace.html>.

Electronic Privacy Information Center - Workplace Privacy Pages <http://epic.org/privacy/workplace/>.

Privacy Rights Clearing House – Workplace Privacy <http://www.privacyrights.org/fs/fs7-work.htm>.

Roger Clarke's Workplace Privacy Resources <http://www.anu.edu.au/people/Roger.Clarke/DV/Workplace.html>.

The National Workrights Institute – Electronic Monitoring <http://www.workrights.org/issue_electronic.html>.