CHAPTER 1

A Thin Wall of Privacy Protection, with Gaps and Cracks: Regulation of Employees' Personal Information and Workplace Privacy in Australia

Anthony Forsyth[*]

§1.01 INTRODUCTION

The protection of employees' personal information and workplace privacy is once again becoming a significant employment law issue in Australia. Rapid technological change in the 1990s resulted in legislative and policy responses in several Australian jurisdictions, amid concerns about growing intrusion upon employees' personal lives. These developments also generated a considerable volume of academic literature.[1] The pace of legal change, and the extent of academic consideration of workplace privacy, slowed to some degree in the 2000s. However the evolution of newer technologies – and their adaptation by employers for purposes including recruitment, surveillance

* Professor, Graduate School of Business & Law, RMIT University, Melbourne, Australia; Consultant, Corrs Chambers Westgarth, Lawyers. Thanks to Alannah Hogan of Corrs Chambers Westgarth for research assistance.

1. See e.g. Ronald McCallum and Greg McCarry, *Worker Privacy in Australia*, 17 Comp. Lab. L. & Policy J. 13 (1996); Richard Johnstone, *Pre-employment Health Screening: The Legal Framework*, 1 Australian J. Labour L. 115 (1988); Anna Chapman and Joo-Cheong Tham, *The Legal Regulation of Information in Australian Labor Markets: Disclosure to Employers of Information about Employees*, 21 Comp. Lab. L. & Policy J. 613 (2000); Ronald McCallum, *Employer Controls over Private Life* (UNSW Press 2000); Julian Sempill, *Under the Lens: Electronic Workplace Surveillance*, 14 Australian J. Labour L. 111 (2001); Ronald McCallum & Andrew Stewart, *The Impact of Electronic Technology on Workplace Disputes in Australia*, 24 Comp. Lab. L. & Policy J. 19 (2002); Margaret Otlowski, *Employers' Use of Genetic Test Information: Is there a Need for Regulation?* 15 Australian J. Labour L. 1 (2002).

and monitoring of employees, and their (mis)use by employees themselves – has seen renewed attention to these issues in the last five years. This is particularly evident in the growing number of court and tribunal decisions examining various aspects of the delicate balance between employer interests in control over the workforce and employees' privacy rights.

Australians have enthusiastically embraced all forms of information and communication technology. One positive effect of this has been to bridge the distance between our 'geographically far-flung nation' and 'the centers of global capital in North America, Europe and Japan'.[2] The use of social media by private citizens in Australia had increased to 62% of the population by 2012 – with much of this access to forums such as Facebook, Twitter and LinkedIn occurring at the workplace and/or using work-provided devices.[3] The interface between social media and the workplace has given rise to a number of employment law issues, including the extent of employers' rights to monitor the activities of employees; and the blurring of 'work' and 'private' life.[4]

Under the Australian federal system of government, regulation of workplace privacy and related employment issues occurs through a complex web of Federal, State and Territory laws. In general terms, the employment of almost all private sector employees is covered by Federal legislation: the *Fair Work Act 2009* (Cth) (*FW Act*). This includes regulation of minimum wages and other employment conditions such as working hours and leave entitlements, either directly (through the National Employment Standards)[5] or indirectly through modern awards and/or enterprise agreements made under the *FW Act*.[6] Federal public sector employees and those in Victoria, the Australian Capital Territory and Northern Territory are also covered by the national system of workplace regulation under the *FW Act*. The employment of public service employees in the remaining five States (New South Wales, Queensland, South Australia, Tasmania and Western Australia) is regulated by specific legislation in each State.[7]

Privacy is the subject of specific Federal legislation applicable to both the private and public sectors nationally: the *Privacy Act 1988* (Cth) (*Privacy Act*). Similar legislation also applies in most Australian States and Territories, regulating the privacy practices of State/Territory public sector organisations in those jurisdictions.[8] In

2. McCallum & Stewart, *supra* n. 1, at 19.
3. M. Watkins et al., *State of Australian Social Media 2012*, quoted in Andrew Bland and Sarah Waterhouse, *Social Media in the Workplace: Practical Tips for Best Practice Policies*, Internet L. Bull. 45 (June 2013). See further Geoffry Holland, Kathryn Crossley & Wenee Yap, *Social Media Law and Marketing: Fans, Followers and Online Infamy* (Thomson Reuters Lawbook Co. 2014).
4. Louise Thornthwaite, *Social Media, Unfair Dismissal and the Regulation of Employees' Conduct outside Work*, 26 Australian J. Labour L. 164 (2013).
5. *FW Act*, Part 2-2.
6. *FW Act*, Parts 2-3 and 2-4 respectively.
7. For example, *Industrial Relations Act 1996* (NSW) and *Public Sector Employment and Management Act 2002* (NSW).
8. *Privacy and Personal Information Protection Act 1998* (NSW); *Information Privacy Act 2009* (Qld); *Personal Information Protection Act 2004* (Tas); *Information Privacy Act 2000* (Vic); *Information Act 2002* (NT). South Australia and Western Australia do not have specific privacy legislation, although some privacy protections are provided by other laws. The Federal *Privacy Act* applies in the Australian Capital Territory.

addition, the common law offers some measure of protection of the privacy rights of individuals; and in some States, further legislation regulates the handling of personal health information.[9] There are also laws in each Australian jurisdiction dealing with prohibitions on illegitimate or unauthorised telecommunications interception and monitoring.[10] Some of these statutes specifically regulate surveillance in the workplace context.[11]

In relation to three specific areas of employment law in which issues of protection of employees' personal information, or breach by employees of their own workplace obligations, commonly arise:

- Unfair dismissal protections are provided by the *FW Act*,[12] and each of the State industrial statutes (although the vast number of unfair dismissal claims are brought under the Federal legislation). An increasing number of unfair dismissal cases involve alleged misconduct by employees using various forms of employer-provided or personally owned technology (e.g., to access social media sites) – often outside the workplace or regular work hours. These cases have raised questions as to the reach of express and implied duties of employees under the contract of employment.[13]
- Protections against employment discrimination and sexual harassment apply under Federal, State and Territory legislation.[14] These laws impose restrictions on employers around the acquisition and use of individuals' personal information as part of recruitment and management processes. Some of the statutes also operate to prevent certain types of discriminatory information requests in the hiring of employees.
- Workplace health and safety (WHS) and workers' compensation for illness or injury are also the subject of Federal, State and Territory laws. Various privacy issues arise in the operation of WHS and workers' compensation legislation, for example in relation to employers' handling of employees' sensitive health information. Although hitherto regulated mainly by WHS laws, workplace bullying has recently become subject to new Federal provisions enabling bullying claims to be initiated by individual employees in the Fair Work

9. *Health Records and Information Privacy Act 2002* (NSW); *Health Records Act 2001* (Vic); *Health Records (Privacy and Access) Act 1997* (ACT).
10. For example *Telecommunications (Interception and Access) Act 1979* (Cth); *Surveillance Devices Act 2004* (Cth); *Invasion of Privacy Act 1971* (Qld); *Listening and Surveillance Devices Act 1972* (SA); *Listening Devices Act 1991* (Tas); *Surveillance Devices Act 1998* (WA); *Surveillance Devices Act 2007* (NT).
11. *Workplace Surveillance Act 2005* (NSW); *Surveillance Devices (Workplace Privacy) Act 2006* (Vic), inserting Part 2A in the *Surveillance Devices Act 1999* (Vic); *Workplace Privacy Act 2011* (ACT).
12. *FW Act*, Part 3-2.
13. Thornthwaite, *supra* n. 4.
14. For example, *Racial Discrimination Act 1975* (Cth); *Sex Discrimination Act 1984* (Cth); *Disability Discrimination Act 1992* (Cth); *Age Discrimination Act 2004* (Cth); *FW Act*, Part 3-1 (ss 351–352); *Equal Opportunity Act 2010* (Vic); *Discrimination Act 1991* (ACT).

Commission (FWC).[15] The management of bullying cases raises privacy issues for employers including the need to maintain the privacy of information provided by the complainant and the alleged 'bully' once a complaint has been made.

In light of the above, it is apparent that larger Australian employers with operations across State/Territory boundaries face an array of overlapping – and at times conflicting – laws imposing obligations in relation to employees' personal information. The absence of uniform regulation in this area across Australia also means that individual employees' expectations of the level of privacy protection in the workplace do not accord with the actual legal position.[16]

§1.02 REGULATORY SCHEMES FOR PROTECTION OF EMPLOYEES' PERSONAL INFORMATION AND PRIVACY

[A] Australian Constitution and State/Territory Human Rights Charters

There is no constitutional or other general right to privacy in Australia. The protection of individual rights under the *Australian Constitution* is quite limited and does not extend to privacy.[17] There is no separate Bill of Rights at the Federal level. Two Australian jurisdictions have enacted human rights charters which include the right to privacy and protection of reputation: *Charter of Human Rights and Responsibilities Act 2006* (Victoria), section 13;[18] and *Human Rights Act 2004* (ACT), section 12.[19] However, the privacy protections offered by both these instruments are restricted in nature. For example, the Victorian Charter:

15. FW Act, Part 6-4B, operative from 1 January 2014. For background see Caroline Kelly, *An Inquiry into Workplace Bullying in Australia: Report of the Standing Committee on Education and Employment* – Workplace Bullying: We Just Want It to Stop, 26:2 Australian J. Labour L. 224 (2013); Sarah Oxenbridge & Justine Evesson, *Bullying Jurisdiction Strategies: An Analysis of Acas' Experience and its Application in the Australian Context*, Report for the Fair Work Commission, Employment Research Australia (July 2013).
16. See e.g. Australian Government, Office of the Australian Information Commissioner, *Guidelines on Workplace E-mail, Web Browsing and Privacy* (March 2000), at: http://www.oaic.gov.au/privacy/privacy-archive/privacy-guidelines-archive/guidelines-on-workplace-email-web-browsing-and-privacy (accessed 8 January 2014); and see further s. §1.06 of this chapter (Conclusion). On workplace privacy protections in Australia in comparative terms – see, e.g. Anne O'Rourke, Amanda Pyman & Julian Teicher, *The Right to Privacy and the Conceptualisation of the Person in the Workplace: A Comparative Examination of EU, US and Australian Approaches*, 23 Int'l J. Comp. Labour L. & Indus. Rel. 161 (2007).
17. Some of the rights protected include the right to vote (*Australian Constitution*, s. 41), the right to trial by jury (s. 80) and freedom of religion (s. 116): see George Williams, *A Charter of Rights for Australia* (UNSW Press, Sydney, 3rd edition, 2007, Chapter 3.
18. This provision states that: 'Everyone has the right—
    (a) not to have his or her privacy, family, home or correspondence unlawfully or arbitrarily interfered with; and
    (b) not to have his or her reputation unlawfully attacked.'
19. Stated in almost identical terms to s. 13 of the Victorian Charter, *supra* n 18.

> does not create any new cause of action for individuals who believe their privacy has been interfered with. Instead, the Charter requires that any bill (new legislation) introduced into the Victorian Parliament must be accompanied by a statement of compatibility with the human rights protected by the Charter. Where the bill is incompatible with one or more of the rights in the Charter, reasons for this must be provided.
>
> The Charter also requires that existing [State] laws are interpreted, as far as is possible, in a way that is compatible with human rights. Further, the Charter imposes an obligation on public authorities [in Victoria] to consider human rights in their decision making and makes it unlawful, in most circumstances, for a public authority to act in a way that is incompatible with a human right.[20]

[B] Common Law Protection of Privacy

While the High Court of Australia affirmed in 1937 that there is no general right to privacy under Australian law,[21] the common law of tort and equitable principles relating to use of confidential information do provide some protection for individuals against privacy breaches. The High Court's more recent decision in *Australian Broadcasting Corporation v. Lenah Game Meats Pty Ltd*[22] is thought by some to provide a stronger basis for equitable actions in particular, and has contributed to debate over the need for a statutory action for breach of privacy in Australia[23] (this debate has been given momentum by the media phone-hacking scandal which led to the Leveson Inquiry in the United Kingdom).[24]

20. Office of the Victorian Information Privacy Commissioner, *Privacy and the Charter of Human Rights and Responsibilities*, Info Sheet 03.08 (June 2008), at: http://www.privacy.vic.gov.au/privacy/web2.nsf/files/privacy-and-the-charter-of-human-rights-and-responsibilities/$file/info_sheet_03_08.pdf (accessed 14 January 2014). Similar limitations apply in the ACT; see Gilbert and Tobin Centre of Public Law, University of NSW, 'The ACT Human Rights Act', at: http://www.gtcentre.unsw.edu.au/node/3074 (accessed 14 January 2014). In relation to the ACT and Victorian human rights charters generally, see Williams, *supra* n. 17, at ch. 5; Simon Evans & Carolyn Evans, *Legal Redress under the Victorian Charter of Human Rights and Responsibilities*, 17 Public Law Review 264 (2006).
21. *Victoria Park Racing and Recreation Grounds Co Ltd v. Taylor* (1937) 58 CLR 479 (owner of racecourse not able to prevent defendants from broadcasting race information from a viewing platform on adjacent land).
22. (2001) 208 CLR 199 (although plaintiff unsuccessful in action seeking to prevent broadcast of film showing its slaughtering practices for meat export, obtained by animal rights campaigners, judgments indicated openness to recognition of tort of invasion of privacy).
23. See e.g. Barbara McDonald, *A Statutory Action for Breach of Privacy: Would It Make a (Beneficial) Difference?* 36 Australian Bar Review 241, 243–250 (2013); Australian Law Reform Commission (ALRC), *For Your Information: Australian Privacy Law and Practice*, ALRC Report No. 108, 2008, discussed in McDonald, *supra* n. 23, at 254–255, 262–268; ALRC, *Serious Invasions of Privacy in the Digital Era*, Issues Paper 43, October 2013.
24. The events in the UK partly precipitated the recent Finkelstein Inquiry into Media and Media Regulation in Australia.

[C] Privacy Protection under Federal Law: The Privacy Act

The *Privacy Act* came into operation in 1988, initially imposing privacy requirements only on Federal public sector departments and agencies in the handling of personal information.[25] In 2001, this framework of privacy regulation was extended to the private sector (although small businesses with an annual turnover under AUD 3 million were exempted).[26] Until March 2014, the *Privacy Act* set down a number of Information Privacy Principles (IPPs) applicable to public sector bodies, and National Privacy Principles (NPPs) for the private sector. The IPPs and NPPs imposed similar obligations in relation to the collection, use, storage and disclosure of 'personal information' by organisations – i.e. information about an individual whose identity was apparent or reasonably ascertainable from that information.[27] In general terms,[28] the IPPs and NPPs required that personal information about an individual:

- could only be collected for a lawful purpose;
- could only be used for that purpose (with some limited exceptions);
- had to be kept in accurate and current records, accessible to the individual concerned (who must also have had the ability to correct their record);
- had to be securely stored;
- could not be disclosed to a third party without the individual's consent (or on certain limited public interest grounds).

Under amendments to the *Privacy Act* which took effect in March 2014, the IPPs and NPPs were replaced by one set of Australian Privacy Principles (APPs) that now apply to Federal government departments/agencies and private businesses.

Additional protections apply under the APPs in relation to 'sensitive information' – i.e. information about an individual's racial or ethnic origin, political opinions or affiliations, religious or philosophical beliefs, membership of a professional body or trade union, sexual preference, criminal record, health information and genetic information.[29]

[D] Employee Records Exemption from the Privacy Act

Importantly, any act or practice directly related to an 'employee record' was excluded from the operation of the NPPs – and this exclusion remains in place under the new

25. Unless otherwise stated, the following discussion of the *Privacy Act* (prior to the 2012 amendments which took effect in March 2014) draws upon McCallum and Stewart, *supra* n. 1, at 32–34; and Carolyn Doyle & Mirko Bagaric, *Privacy Law in Australia*, Federation Press, Sydney, 2005, 99, 119–129, 153–155. Note also relevant State and Territory privacy legislation, *supra* n. 8..
26. *Privacy Amendment (Private Sector) Act 2000* (Cth).
27. *Privacy Act*, s. 6(1) (definition of 'personal information').
28. For further detail see Jeremy Douglas-Stewart, *Annotated National Privacy Principles* (4th ed., Presidian Legal Publications 2009).
29. *Privacy Act*, s. 6(1) (definition of 'sensitive information').

APPs.[30] This means that private sector employers are *not* subject to the limits on the collection, use, storage and disclosure imposed by the APPs, in respect of any 'record of personal information relating to the employment of [an] employee'.[31] This includes an employee's health information, and personal information relating to the employee's:[32]

- engagement, training, discipline or resignation;
- termination of employment;
- terms and conditions of employment;
- personal and emergency contact details;
- performance or conduct;
- hours of work, salary or wages;
- membership of a professional body or trade union;
- recreation, long service, sick, personal, maternity, paternity or other leave;
- taxation, banking or superannuation (i.e. pension) affairs.

The employee records exemption from the *Privacy Act*, and its application in a number of specific employment contexts (e.g., monitoring of employee emails and internet use) are discussed further in the remainder of this chapter. For now, it should be noted that the exemption has long been a controversial aspect of Australia's privacy regime.[33] The main justification for exempting employee records from the *Privacy Act* was that privacy protection for employees 'is more properly a matter for workplace relations legislation'.[34] However, several reviews and inquiries over the last fifteen years have identified significant limitations in the privacy protections provided to employees under Federal, State and Territory workplace laws.[35] According to Otlowski:

> Inclusion of the broad exemption in the [*Privacy Act*] for employee records consequently leaves employees vulnerable to breaches of privacy at the hands of their employers, in respect of which they would not necessarily have a remedy.[36]

30. *Privacy Act*, s. 7B(3).
31. *Privacy Act*, s. 6(1) (definition of 'employee record'). However, the employee records exclusion does not apply in the public sector; therefore, Federal government departments and agencies must observe the requirements of the APPs in their handling of employees' personal information.
32. *Ibid*.
33. See e.g. the criticism in Senate Legal and Constitutional References Committee, *Privacy in the Private Sector: Inquiring into Privacy Issues, including the Privacy Amendment Bill 1998*, 1999, discussed in Margaret Jackson, *Hughes on Data Protection in Australia* 109 (2d ed., Lawbook Co 2001).
34. Margaret Otlowski, *Employment Sector By-Passed by the Privacy Amendments*, 14 Australian J. Labour L. 169, 172 (2001) (see also 174).
35. See e.g. House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000*, 2000, discussed in Otlowski, *supra* n. 34, at 172–175; Victorian Law Reform Commission, *Workplace Privacy: Final Report*, Victorian Government Printer, Melbourne, 2005, Chapter 2; ALRC (2008), *supra* n. 23.
36. Otlowski, *supra* n. 34, at 175. See also Doyle and Bagaric, *supra* n. 25, at 153–154.

A wide-ranging review of the *Privacy Act* by the ALRC in 2008 included recommendations for the removal of the employee records exclusion on the following grounds:

> While public sector agencies are required to treat employee records in accordance with the *Privacy Act*, private organisations generally are exempt in relation to current and past employees (with some limited exceptions). There seems little justification in principle for the differential approach—which does not feature in the law of comparable jurisdictions.
>
> The ALRC recommends that this exemption be removed. This would create consistent rules for personal information about employees, regardless of whether they are public or private sector employees.
>
> The ALRC acknowledges that there may be circumstances in which it is undesirable to allow employees to have access to all of the information contained in their files—such as referees' reports and other similarly confidential material. It would be much better practice to deal with such exceptions on the basis of the general law of confidentiality, however, rather than wholly exempting private sector employers from the normal requirements of the *Privacy Act*.[37]

[E] 2012 Amendments to the Privacy Act

The ALRC's 2008 Review of the *Privacy Act* ultimately lead to passage of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) (*Privacy Amendment Act*). This legislation made extensive changes to the *Privacy Act*, which took effect on 12 March 2014. The most significant aspects of the *Privacy Amendment Act* for present purposes are:[38]

- enhancement of the Federal Privacy Commissioner's powers to ensure compliance with the *Privacy Act*, including civil penalties of up to AUD 340,000 for individuals and AUD 1.7 million for organisations (in instances of serious or repeated breach of an individual's privacy); and
- adoption of the APPs for both the public and private sectors. In terms of content, the APPs impose very similar privacy obligations to those which previously applied under the IPPs and NPPs.

---

37. ALRC (2008), *supra* n. 23, at Executive Summary; note also the following Recommendations in the ALRC's Report:
    > Recommendation 40–1 The *Privacy Act* should be amended to remove the employee records exemption by repealing s 7B(3) of the Act.
    >
    > Recommendation 40–2 The Office of the Privacy Commissioner should develop and publish guidance on the application of the model Unified Privacy Principles to employee records, including when it is and is not appropriate to disclose to an employee concerns or complaints by third parties about the employee.
38. See Norman Witzleb, *Halfway or Half-Hearted? An Overview of the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)*, 41 Australian Bus. L. Rev. 55 (2013); Alec Christie, *The Australian Privacy Act Amendments Will Significantly Impact Federal Government Agencies*, Priv. L. Bull. 49 (December 2013).

Table 1.1 Summary of the Australian Privacy Principles (Effective 12 March 2014)[39]

APP1	*Organisations must maintain a clear policy on management of personal information*
APP2	Individuals may interact with organisations anonymously or using a pseudonym
APP3	Organisations may collect sensitive information only where an individual consents and the information is reasonably necessary for the agency's activities/functions, or collection is authorised by law
APP4	Obligations of organisations in relation to unsolicited personal information
APP5	Organisations must notify individuals about collection of personal information
APP6	Sensitive information must only be used for the primary purpose for which it was collected (although use for some secondary purposes is permitted)
APP7	Prohibition of use of personal information for direct marketing
APP8	Requirements relating to cross-border disclosure of personal information by organisations
APP9	Restrictions on use of government related identifiers of individuals
APP10	Organisations must ensure that personal information collected is accurate, up to date and complete
APP11	Obligations of organisations to ensure security of personal information (i.e. prevent misuse, interference, unauthorised access, etc.)
APP12	Right of individuals to access personal information about them held by an organisation
APP13	Obligation of organisations to correct personal information which is inaccurate, out of date, misleading, etc.

However, as mentioned earlier, no change has been made to the employee records exemption from the *Privacy Act* (although the former Labor Federal Government indicated that this could arise from a second stage legislative response to the ALRC's 2008 privacy law review).[40]

39. For the full text of the APPs see Australian Government, Office of the Australian Information Commissioner, *Australian Privacy Principles*, Privacy Fact Sheet 17, January 2014, at: http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles (accessed 8 January 2014).
40. See Witzleb, *supra* n. 38, at 55; Helen Lewin, *Australian Law Reform Commission's Report on Australian Privacy Law* – For Your Information: Australian Privacy Law and Practice, Keeping Good Companies 543 (October 2008). Note however that the prospect of amendment to the

[F] Remedies under the Privacy Act

In addition to the new civil penalties for serious privacy breaches, the remedies available under the *Privacy Act* include:

- a right for individuals to lodge a complaint with the Privacy Commissioner, which has investigatory and evidence-gathering powers;[41]
- the availability of compensation and other declaratory remedies (e.g. a declaration that conduct constituting an interference with an individual's privacy has occurred and should not be repeated, or that the respondent take any reasonable action to redress the loss or damage suffered by the complainant), as part of a determination issued by the Privacy Commissioner following an investigation into an alleged privacy breach;[42]
- an injunction to restrain a privacy breach, following an application to the Federal Court or Federal Circuit Court by the aggrieved party or the Privacy Commissioner.[43]

§1.03 PERSONAL INFORMATION PROTECTION IN THE HIRING PROCESS

[A] Overview

A range of restrictions apply to Australian employers' ability to request, use and retain information about prospective employees in the recruitment process. These limits derive from several different sources, including anti-discrimination laws, spent convictions legislation and the *Privacy Act*.

Employers are permitted to request a job applicant's address, telephone number and e-mail address when he/she applies for a position. There is no legal basis for an employer to insist that a prospective employee provide his/her social network password in the recruitment process. However, many employers now carry out searches of job applicants' publicly accessible social media presence to identify any negative personal activities or behaviour.[44] A recent ALRC Issues Paper canvasses the idea of

---

current employee records exemption has most likely narrowed, following the election to office of the (conservative) Coalition Government in September 2013.

41. *Privacy Act*, ss 36 and 40. Since 12 March 2014, the Privacy Commissioner also has the power to initiate investigations on its own motion: Charles Alexander, Elizabeth Koster & Helen Paterson, *Punitive Powers Guided by Ambiguity: The Australian Federal Privacy Commissioner's New Powers in the Context of a Principles-based Privacy Regime*, Priv. L. Bull. 66, 67–68 (January 2013).
42. *Privacy Act*, s. 52; see e.g. *Rummery v. Federal Privacy Commissioner* [2004] AATA 1221. Enforcement of determinations issued by the Privacy Commissioner requires proceedings to be brought in the Federal Court of Australia or the Federal Circuit Court.
43. *Privacy Act*, s. 98.
44. See e.g. CCH, *Australian Privacy Reporter*, CCH Australia Ltd, 2012, [20-216]; Lucille Keen, *#bored at Work Means #yourefired*, Australian Fin. Rev. 1, 6 (13 January 2014); Thornthwaite, *supra* n. 3, at 168.

prohibiting employer requests for access to job applicants'/employees' private social media accounts, noting that a number of United States jurisdictions have passed legislation to that effect.[45]

[B] Application of the Privacy Act to Recruitment/Hiring

The collection of the above or any other types of personal information in the course of an individual's employment application *is* subject to the protections in the *Privacy Act*, including the requirements of the APPs. This is because the employee records exemption from the *Privacy Act* does not apply in the pre-employment context[46] – it only applies to current and former employment relationships[47]. As a result, employers must ensure compliance with the *Privacy Act* during the hiring process, for example by:[48]

- telling job applicants how their personal information (e.g. in their curriculum vitae) will be collected from them, and from third parties such as referees;
- collecting that information in a fair and non-intrusive manner;
- only collecting information that is relevant to the individual's application for the particular position;
- allowing the applicant access to their personal information on request (this can also extend to the employer's files relating to the application, including interview notes although not third party references[49]).

[C] Anti-discrimination Law Provisions

Legislation in every Australian jurisdiction prohibits discrimination against individuals in the advertising and offering of employment.[50] Some Federal and State anti-discrimination statutes contain further provisions precluding employers from making certain kinds of requests for information from prospective employees.[51] At the Federal level, such requests are prohibited where the information requested is in connection with, or for the purposes of, unlawful discrimination on the basis of a person's sex, disability or age; and persons without that attribute would not be asked to provide the

45. ALRC (2013), *supra* n. 23; 'ALRC to consider ban on employer request for Facebook passwords', *Workforce*, No 18912, 29 October 2013.
46. Doyle & Bagaric, *supra* n. 25, at 155; note also *Privacy Act*, s. 6(1) (definition of 'employee record'), *supra* n. 31, referring to records 'relating to the employment of the employee'.
47. *Privacy Act*, s. 7B(3), *supra* n. 30.
48. CCH, *supra* n. 44, at [20-210].
49. See *O v. Automotive Company* [2009] PrivCmrA 18.
50. See e.g. *supra* n. 14.
51. See Chapman & Tham, *supra* n. 1, at 629–634; Neil Rees, Katherine Lindsay & Simon Rice, *Australian Anti-discrimination Law: Text, Cases and Materials* 443–444 (Federation Press 2008).

same information.[52] These provisions would therefore prevent an employer from making verbal requests (e.g. at a job interview) for information about an applicant's:

- gender, sexual orientation, gender identity, intersex status, marital or relationship status, pregnancy or potential pregnancy, breastfeeding or family responsibilities;[53]
- age or age group;
- disability (including a physical or mental disease, disorder or illness), although questions may be asked about a person's ability to perform the inherent or reasonable requirements of the position he/she is seeking;[54] in turn, this may inform the employer's consideration of the reasonable adjustments that may be necessary to accommodate the individual in the workplace.[55]

The above prohibitions would also apply to requests for information of this nature in written form, for example on a job application or medical form.

In Queensland and Victoria, employer requests from job applicants for information that would form the basis of unlawful discrimination are prohibited.[56] This would cover information relating to a prospective employee's sex, age or disability (as per Federal anti-discrimination statutes); as well as information about the individual's race, physical features, political/religious belief or activity, or industrial activity (e.g. union membership).

[D] Health Screening

Employers commonly request prospective employees to answer questions about their health, or even undergo a medical examination, as part of the recruitment process. Such requests are lawful; however, a job applicant cannot be compelled to provide health information, and his/her participation in any health screening (including genetic testing, such as for susceptibility to workplace hazards) must be voluntary.[57] In

52. *Sex Discrimination Act 1984* (Cth), s. 27; *Disability Discrimination Act 1992* (Cth), s. 30; *Age Discrimination Act 2004* (Cth), s. 32.
53. See e.g. *Smith v. Commonwealth of Australia* (2000) EOC 93-077. However, under s. 27(2) of the *Sex Discrimination Act 1984* (Cth), job applicants may be asked about medical information concerning their pregnancy; or any gender-specific medical conditions.
54. See Rees, Lindsay & Rice, *supra* n. 51, at 283–287, including extract from *X v. Commonwealth* (1999) 200 CLR 177 (Australian Army soldier discharged after positive HIV test during training; High Court upheld Army's argument re inherent requirement that soldier not pose risk of HIV transmission to other soldiers).
55. Chapman & Tham, *supra* n. 1, at 634; Otlowski, *supra* n. 1, at 14.
56. *Equal Opportunity Act 2010* (Vic), s. 107; *Anti-Discrimination Act 1991* (Qld), s. 124. See e.g. *Bair v. Goldpath* [2010] QCAT 483 (job applicant was unlawfully asked questions about his age, parental leave status and sick leave history at previous employer; however, only a written apology was ordered rather than compensation or damages).
57. Otlowski, *supra* n. 1, at 3–9. See further David Keays, *The Legal Implications of Genetic Testing: Insurance, Employment and Privacy*, 6 J. L. & Med. 357 (1999); and the reform proposals outlined in ALRC, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC Report 96, March 2013.

contrast, employers have the power at common law to direct an existing employee to undergo a medical examination to determine the employee's fitness for duties (as long as the direction is reasonable in the circumstances).[58]

Employers also need to be mindful of anti-discrimination laws when conducting pre-employment medical checks.[59] For example, if a check is being conducted to establish whether an individual has a higher propensity to make workers' compensation claims, employers must exercise caution as this could indicate an intention to make a decision not to employ the person which constitutes unlawful discrimination on the grounds of disability or impairment.[60] However, legislation in Queensland specifically allows employers to require a prospective employee to disclose a pre-existing injury or medical condition upon request by an employer; and to access the prospective employee's workers' compensation claim history (where the individual consents).[61]

Under the *Privacy Act*, as any 'health information'[62] provided by a job applicant is considered sensitive personal information, and the employee records exemption from the *Privacy Act* does not apply in the pre-employment context (*supra*), that information must be handled by the employer in accordance with the APPs (noting the stronger protections which they provide for sensitive information).[63]

[E] Criminal Records

Having become widespread over the last fifteen years,[64] criminal record checks on prospective employees are regulated by the *Privacy Act* and spent convictions legislation operating in all Australian jurisdictions except Victoria. Under the *Privacy Act*, information relating to a person's criminal record is considered sensitive information to which the APPs and additional protections apply. An employer can run a criminal

58. Breen Creighton & Andrew Stewart, *Labour Law* 407 (5th ed., Federation Press 2010) referring to *Blackadder v. Ramsey Butchering Services Pty Ltd* (2002) 113 IR 461; see also *Schoeman v. Director-General, Department of Attorney-General and Justice* [2013] NSWIR Comm 108.
59. See further Otlowski, *supra* n. 1, at 9–20; Wendy Zukerman, *Genetic Discrimination in the Workplace: Towards Legal Certainty in Uncertain Times*, 16 J. L. & Med. 770 (2009).
60. Andrew Stewart, *Stewart's Guide to Employment Law* 86 (4th ed., Federation Press 2013). See e.g. *Own Motion Investigation v. Australian Government Agency* [2007] PrivCmr A 4 (government body which sought information about work-related injuries/illness in recruitment process, settled Privacy Commissioner's investigation by agreement to review selection process and remove offending questions).
61. *Workers' Compensation and Rehabilitation and Other Legislation Amendment Act 2013* (Qld), amending the *Workers' Compensation and Rehabilitation Act 2003* (Qld).
62. As defined in s. 6(1), including information about an individual's health or disability; information about a health service provided to an individual; and other personal information about an individual collected in connection with donation by the individual of his/her body parts, organs or substances.
63. See further Doyle & Bagaric, *supra* n. 25, at 157–160.
64. Criminal record checks in Australia increased seven-fold in the decade to 2007: see Bronwyn Naylor, Moira Paterson & Marilyn Pittard, *In the Shadow of a Criminal Record: Proposing a Just Model of Criminal Record Employment Checks*, 32 Melbourne U. L. Rev. 171, 172 (2008). See also Moira Paterson & Bronwyn Naylor, *Australian Spent Convictions Reform: A Contextual Analysis*, 34 UNSW L. J. 938 (2011).

record check on an individual through the official authorities (e.g. Australian Federal Police), if the individual consents.[65] In practice, an individual him/herself will usually request a criminal record report from the relevant authority, then provide it to the prospective employer.

Where a prior criminal conviction constitutes a 'spent conviction' under the terms of applicable Federal, State or Territory legislation,[66] it does not have to be disclosed by a prospective employee. Further, these laws 'forbid employers … from taking into account spent convictions in making assessments about [the] character and fitness' of a job applicant.[67] The definition of a spent (or lapsed) conviction varies across jurisdictions. Generally, however, offences that are more than 10 years old (or 5 years old for young offenders) – and carry low maximum jail terms (e.g. 6 months in NSW, Tasmania, ACT and NT; 30 months in Queensland and federally) – will be considered spent convictions for purposes of the applicable legislation.[68] A number of exclusions apply, for example requiring persons convicted of violent/sex offences to disclose these when seeking employment involving children (in fact 'working with children checks' are mandatory for such employment across Australia).[69]

Discrimination on the basis of an irrelevant criminal record (i.e. not relevant to a person's ability to perform a particular job) is also unlawful under Federal, Tasmanian and NT legislation.[70] Allegations of unlawful discrimination on the basis of a person's criminal record are fairly common, making up 23% of complaints to the Federal Human Rights and Equal Opportunity Commission (HREOC) under the *AHRC Act* in 2010-2011.[71] In response, the HREOC has issued guidelines indicating that employers should not ask job applicants or employees about any past criminal convictions, unless this information is relevant to the individual's ability to perform the inherent requirements of the particular position (e.g. a prior driving offence may be relevant where a driver's licence is required to perform the job; a prior offence involving dishonesty may be relevant where the job involves responsibility for financial matters).[72]

65. Private organisations offering criminal record check services can also be used only with the prospective employee's consent: Moira Paterson, *Restrictions on Employers' Handling of Criminal Records Information: Privacy and Confidentiality Issues*, 18:8 Empl. L. Bull. 120, 121 (2012).
66. *Crimes Act 1914* (Cth), Part VIIC; *Criminal Records Act 1991* (NSW); *Criminal Law (Rehabilitation of Offenders) Act 1986* (Qld); *Spent Convictions Act 2011* (SA); *Annulled Convictions Act 2003* (Tas); *Spent Convictions Act 1988* (WA); *Spent Convictions Act 2000* (ACT); *Criminal Records (Spent Convictions) Act 1992* (NT).
67. Paterson, *supra* n. 65, at 121.
68. *Ibid*.
69. See e.g. Department of Justice, Victoria, 'Working with Children Check' at: http://www.workingwithchildren.vic.gov.au/home/applications/the+application+process/what+is+checked/ (accessed 20 January 2014); CCH, *Australian Human Resource Management*, CCH Australia Ltd, 2012, [5-890].
70. *Australian Human Rights Commission Act 1986* (Cth) (*AHRC Act*), s. 3(1) and *Australian Human Rights Commission Regulations 1989* (Cth), regulation 4; *Anti-Discrimination Act 1998* (Tas), s. 50; *Anti-Discrimination Act 1992* (NT), s. 4.
71. HREOC, *Discrimination in Employment on the basis of Criminal Record* at: http://www.humanrights.gov.au/discrimination-employment-basis-criminal-record (accessed 20 January 2014).
72. HREOC, *On the Record: Guidelines for the Prevention of Discrimination in Employment on the basis of Criminal Record* 5, 14–19, 2012, at: http://www.humanrights.gov.au/sites/default/

Finally, even where spent convictions or anti-discrimination laws would otherwise apply, licensing and registration requirements in certain industries/occupations require employers both to ask prospective employees about prior criminal activity; and to take that information into account when deciding whether to employ the person. Areas of employment where these specific regulatory arrangements apply include teaching, nursing, policing, correctional and security services, taxis/transport, casinos/gaming/racing, and the legal profession.[73]

§1.04 PERSONAL INFORMATION AND PRIVACY PROTECTION DURING THE EMPLOYMENT RELATIONS

[A] Overview

Australian employers are entitled to obtain a range of personal information relating to their employees, given the employee records exclusion from the *Privacy Act*. However, it is important to understand the limitations of that exclusion and the questions that arise about its application to the monitoring of employee emails, internet use, social media activity, etc. (both while on-duty and outside the workplace/work hours). Legislation regulating various forms of surveillance of employees is also relevant in this context, along with the law impacting on workplace drug and alcohol testing. Misuse by employees of social media – and employers' rights to discipline and dismiss employees on this basis – has become a major issue in Australian employment law recently, giving rise to increasing numbers of unfair dismissal claims. Finally, under the *FW Act*, employers are required to maintain records of employees' pay and other employment conditions for compliance purposes.

[B] Operation of the Privacy Act Employee Records Exemption during Employment

As indicated earlier in this paper, any act or practice directly related to an employee record is exempt from the requirements of the *Privacy Act* (in relation to private sector employers with an annual turnover of at least AUD 3 million). It has also been shown that this exclusion only applies in the context of a current or former employment relationship (therefore, it does not apply in respect of job applicants; nor does it apply in relation to persons engaged as contractors or subcontractors).[74]

---

files/content/human_rights/criminalrecord/on_the_record/download/otr_guidelines.pdf (accessed 20 January 2014), including discussion of *Christensen v. Adelaide Casino Pty Ltd*, unreported (casino's rejection of application for employment as a bar attendant from individual with prior conviction for stealing alcohol seven to eight years previously, found not sufficiently connected to inherent requirements of particular position including requirement of trustworthiness).

73. *Ibid*., 13, 32–33.

74. On the privacy rights of workplace contractors see Leanne Nickels & Rachael Smith, *The Legal Risks Arising from Electronic Storage of Work Information in the Construction Industry*, Mondaq Bus. Briefing (7 June 2012), at: http://www.mondaq.com/ (accessed 7 January 2014).

There are two further requirements that must be satisfied for the exemption in section 7B(3) to apply:

- the act or practice must be directly related to the employment relationship – therefore, use by an employer of personal information contained in an employee record for a purpose extraneous to the employee's employment would not be covered by the exclusion (e.g. the employer's provision of the personal information to a direct marketing firm or debt collection agency; or disclosure of an employee's status as a client of the employer, a charity, without the employee's consent);[75]
- the act or practice must be directly related to the employee record held by the employer – so, for example, if personal information in an employee record is provided by the employer to its workers' compensation insurer, the information does not retain its exempt status in the hands of the insurance company (i.e. the insurer's handling of that information is subject to the APPs in the *Privacy Act*).[76]

The application of the *Privacy Act* (and the employee records exemption) to employers' monitoring of employee email and internet use is discussed in the next section.

[C] Workplace Surveillance/Monitoring of Employees

Australian employers (like employers elsewhere) have a strong interest in monitoring their employees' use of workplace email and the internet, for example 'to ensure that employees are not wasting time or their employer's resources, or harassing co-workers, or even engaging in unlawful activities …'.[77] However, the lawfulness of such monitoring is a complex issue, involving the potential application of the *Privacy Act* and Federal, State and Territory surveillance legislation.[78]

[1] Privacy Act Regulation of Monitoring

In relation to the *Privacy Act*, the first issue to consider is whether an employee's work emails or records of their internet activity constitute 'personal information' which is covered by the protections in the legislation – i.e. do the emails or web records contain information which could in some way enable identification of the individual? This will

75. CCH, *supra* n. 44, at [20-200]–[20-205], including discussion of *B v. Cleaning Company* [2009] PrivCmrA 2 and *C v. Charity* [2011] PrivCmrA 3.
76. CCH, *supra* n. 44, at [20-200]; see also [20-205] noting that this principle applies in respect of the full range of third parties to which an employer may provide employees' personal information for HR management purposes, including payroll processing, medical checks/health services, remuneration consultants, superannuation funds, etc.
77. Creighton & Stewart, *supra* n. 58, at 577.
78. See generally Anne O'Rourke, Julian Teicher & Amanda Pyman, *Internet and Email Monitoring in the Workplace: Time for an Alternate Approach*, 53 J. Indus. Rel. 522 (2011).

often be the case, for example where an employee's name forms part of their email address.[79]

Second, it must be determined whether the employee's emails or web history form part of an employee record and are therefore subject to the *Privacy Act* exemption. This will not always be straightforward. In Creighton and Stewart's view: 'Arguably … information gathered by or accessible to an employer regarding personal e-mails sent on work computers would fall outside the exemption, as would records on internet browsing.'[80] If the contents of an email are not relevant to the employee's employment, then the exemption will not apply.[81] However, according to Banks et al., the *Privacy Act* definition of 'employee record' is broad enough to cover 'many matters of interest to an employer when conducting email surveillance, so as to exclude such emails … from any protection under the legislation' (including information that may ultimately be relevant to disciplinary matters).[82]

In *Griffiths v. Rose*,[83] an employer's monitoring of an employee's use of a work-provided laptop was found not to be inconsistent with the *Privacy Act*. The employee was dismissed by a Federal government department for viewing pornography on the laptop at his home, in breach of the department's IT policy. This followed monitoring by the department using 'Spector 360' technology, which is:

> a utility … known as a 'desktop logging system'. It performed a number of functions including logging the occurrence of particular keywords and taking a precise snapshot of the user's desktop every 30 seconds. … Spector360 also collected all emails, attachments, internet searches and instant messages performed by a user and sent them to [a] dedicated server.[84]

Perram J of the Federal Court found that the department was entitled to insist on the employee's compliance with its IT policy; and its monitoring of his computer use (even at home) to ensure compliance was for a lawful purpose under the *Privacy Act*. The employee's argument that it was unfair for the department to monitor his private use of the laptop was dismissed by Perram J:

> Unlike the circumstance where Spector360 gratuitously collects personal banking information or credit card details during periods of personal use (which may very well involve a breach of privacy) what it collected from Mr Griffiths was the very thing it was intended to collect, namely, evidence of breaches of the Code of Conduct. It was also the very thing the Department had warned Mr Griffiths that it

79. CCH, *Australian Labour Law Reporter*, CCH Australia Ltd, 2012, 31-700.
80. Creighton & Stewart, *supra* n. 58, at 577. See also Dan Svantesson, *Can You Read an Employee's Private Email? Addressing the Legal Concerns*, 12:7 Internet L. Bull. 98 (2009); and Australian Government, Office of the Australian Information Commissioner, *supra* n. 16, asserting that the *Privacy Act*: '… applies to staff e-mails that contain personal information other than "employee records" in certain circumstances. [It] also applies to logs of staff web browsing activities.'
81. CCH, *supra* n. 78, at 31-700.
82. Dianne Banks, Peter Leonard, James Pomeroy, Grace Keesing & Kim McGuren, *Employer Surveillance of Employee Emails: What Are the Rules?* Internet L. Bull. 8, 11(April/May 2013); see also Des Butler and Vanessa Mellis, *Email: Do Employees Have a Right to Privacy?* 23 Queensland Law. 78, 82 (2002).
83. (2011) 192 FCR 130.
84. *Ibid.*, [3].

> was going to monitor his use to detect. In those circumstances, I conclude that the collection of this particular information was not unfair within the meaning of [IPP] 1(2). It is not unfair to warn a person that their computer use will be monitored in order to detect any accessing of pornography and then to do so.[85]

However given the risk that monitoring of employees' emails, in particular, will likely result in some private information being viewed, private sector employers are often counselled to err on the side of compliance with the APPs in the handling of such material (e.g. by keeping access to it within reasonable limits and not using it for ulterior purposes).[86]

Another response to the legal minefield for employers in this area is the widespread adoption of workplace policies on email and internet use, to ensure that employees are aware of an organisation's rules and expectations and the consequences of any misuse (including disciplinary action or dismissal). These policies should also clearly indicate to employees the nature of any monitoring conducted by the employer, and identify relevant personnel who may access staff email and internet records.[87]

[2] Monitoring and Surveillance Legislation

In addition to the *Privacy Act*, email and internet monitoring is subject to the operation of various surveillance legislation in place around Australia, which also regulate other forms of surveillance including telephone monitoring and GPS tracking.

As indicated earlier in this chapter, each Australian jurisdiction has legislation prohibiting unlawful telecommunications interception and monitoring, with some of these laws dealing specifically with workplace surveillance.[88] Many of these statutes were introduced in response to technological developments such as tape recorders and other listening devices (from the 1970s), CCTV cameras (1980s-1990s) and mobile phones (1990s-2000s) – although mostly they pre-date newer technologies like smart phones, tablets and GPS tracking.[89] Employers increasingly deploy these different types of technology for reasons including protecting the business from theft or damage, ensuring compliance with regulatory requirements (e.g. under WHS legislation), monitoring employee performance and observing any misconduct by employees.[90]

---

85. *Ibid.*, [30]. See also *Queensland Rail v. Wake* (2006) 156 IR 393; *B, C and D v. Australian Postal Corporation* [2013] FWCFB 6191.
86. McCallum and Stewart, *supra* n. 1, at 37; see also Margaret Jackson, *A Practical Guide to Protecting Confidential Business Information* 81(Thomson Lawbook Co. 2003).
87. Australian Government, Office of the Australian Information Commissioner, *supra* n. 16. See also Dean Ellinson, *Employees' Personal Use of Their Employer's E-mail System*, 29 Australian Bus. L. Rev. 165 (2001); and *Australian Municipal, Administrative, Clerical and Services Union v. Ansett Australia Limited* (2000) 175 ALR 173, urging employers to adopt policies on acceptable email and IT use.
88. See *supra* nn. 10–11.
89. See Sempill, *supra* n. 1, at 111–115; Chapman & Tham, *supra* n. 1, at 634; Anna Johnston & Myra Cheng, *Electronic Workplace Surveillance, Part 2: Responses to Electronic Surveillance – Resistance and Regulation*, Priv. L. & Policy Reporter 7 (2003); Suzanne Cusack, *Employee Privacy in the Modern Workplace*, 7:3 Priv. L. Bull. 38 (2010).
90. Chapman & Tham, *supra* n. 1, at 634–635.

Federal legislation, the *Telecommunications (Interception and Access) Act 1979* (Cth), will apply in most instances to require that employers notify employees of any interception (i.e. listening or recording) of communications in the workplace such as phone calls or emails.[91] Failure to comply with the requirements of this legislation, for example where an employer intercepts a communication without an employee's knowledge, constitutes a criminal offence.[92] Employers usually seek to ensure compliance with the *Telecommunications (Interception and Access) Act* by informing employees of any intended surveillance of emails or other communications in a workplace policy.[93]

State and Territory statutes also apply to prohibit the use of various types of 'devices' to listen in on private conversations and activities, although some legislation permits a person to record a conversation which he/she is party to or where necessary to protect his/her lawful interests.[94] These laws (some of which also cover video surveillance and GPS tracking) are increasingly coming into play in workplace disputes, with employees covertly recording disciplinary meetings or conflicts with other workers and seeking to rely on the 'evidence' obtained in subsequent legal proceedings.[95] In one recent case, an employee's alleged use of a listening device to record unfair dismissal conciliation proceedings in the FWC led to a police investigation.[96] In another case, the employer's surveillance of an employee was called into question

91. CCH, *supra* n. 44, at [20-300]; see also [20-440] for a detailed discussion of the *Telecommunications (Interception and Access) Act 1979* (Cth).
92. Banks et al., *supra* n. 81, at 10.
93. *Ibid*.
94. For a detailed explanation of the relevant statutes see Doyle & Bagaric, *supra* n. 25, at 142–148; CCH, *supra* n. 44, at [20-440].
95. William Houston, *Covert Recordings? – There's an App for That!*, Baker & McKenzie, *HReSource*, 7 November 2013, discussing *Thomas v. Newland Food Company* [2013] FWC 8220 (employee's secret recording of discussions with management, although legal under Queensland statute, breached trust between parties such that employee not entitled to reinstatement following finding of unfair dismissal: 'there could hardly be an act which strikes at the heart of the employment relationship, such as to shatter any chance of re-establishing the trust and confidence necessary to maintain that relationship, than the secret recording by an employee of conversations he or she has with management'); *Thompson v. John Holland Group Pty Ltd* [2012] FWA 10362 (dismissal of employee for covertly recording discussion about duties, in breach of WA legislation, upheld as breach of company's Code of Ethics requiring employees to protect individuals' privacy); *Hazlam v. Fasche Pty Ltd* [2013] FWC 5593 (recording potentially illegally obtained by employee not admitted in evidence in unfair dismissal case); and *Wintle v. RUC Cementation Mining Contractors Pty Ltd* [2013] FCCA 694 (evidence inadvertently recorded admitted in general protections claim). Note also the observation of Drake DP in *Lever v. Australian Nuclear Science and Technology Organisation* [2009] AIRC 784 [103]: 'Applying ordinary Australian community standards I do not accept that any employee or any employer would be content to have any meeting they were attending secretly tape recorded. The ordinary conduct of personal, business and working relationships in our community is predicated on the basis that if there is to be any record of a meeting it will be agreed in advance. Anything else is quite properly described as sneaky. It's [sic] very sneakiness makes it abhorrent to ordinary persons dealing with each other in a proper fashion.'
96. *Worker Ordered to Pay $10,000 Costs, as Employer Alleges Proceedings Bugged*, Workplace Express, (13 December 2013); Matthew Stevens, *Qube, Lunt and a Little Black Box*, Australian Fin. Rev. 28 (13 December 2013).

although found to be lawful.[97] The potential for unlawful surveillance has also arisen in the context of FWC's role in approving proposed enterprise agreements.[98]

Specific workplace surveillance legislation in several States and the ACT goes further in protecting employees' privacy than the telecommunications interception and listening devices laws already discussed in this chapter. The most comprehensive statute is the *Workplace Surveillance Act 2005* (NSW), which applies to computer surveillance (including employees' email and internet usage, at work or at any other place where work is being performed); video surveillance; and location tracking.[99] Generally, employees must be informed at least fourteen days in advance of any proposed surveillance, including the kind of surveillance that will be carried out; the method to be used; when it will commence; and whether it will be for a fixed period, intermittent or ongoing. Additional notice requirements apply to camera surveillance (e.g. clearly visible signs and cameras), and tracking surveillance (e.g. clearly visible notice on a vehicle). Certain types of surveillance are completely prohibited (e.g. in change rooms, toilets or showers at a workplace; or computer use outside the workplace, unless an employee is using employer-provided equipment). Any records obtained by an employer through any of the types of surveillance permitted by the NSW legislation can only be used for a legitimate purpose related to the employment of employees; the employer's legitimate business activities; or law enforcement purposes. The legislation also includes some restrictions on employers' blocking of employees' email or access to internet sites (e.g., this must be consistent with the employer's workplace surveillance policy).

In Cusack's view, the NSW *Workplace Surveillance Act* has been 'a great step forward in recognising that surveillance in an employment context is very different to surveillance outside of work'; and bridges the gap left by the telecommunications interception and listening devices laws which 'largely rely on … protecting "private conversations" … [but fail] to take into account the employer/employee relationship, and the tension between the need and desire for business to harness technology and the need for reasonable employee privacy.'[100]

97. *Diehm v. Toll Transport Pty Ltd* [2012] FWA 8818 (employer's video surveillance of employee undertaking private activities to ascertain veracity of worker's compensation claim, held legitimate because employee was on paid leave, although dismissal of employee found unfair on other grounds). See also *Claypole v. BlueScope Steel Ltd, JKC v. BlueScope Steel Ltd* [2008] AIRC 276 and 354; *Gervasoni v. Rand Transport (1986) Pty Ltd* [2010] FWAFB 2526.
98. See e.g. *City of Joondalup* [2013] FWCA 7977 (agreement approved despite including clause permitting installation of GPS tracking devices on work vehicles or equipment; FWC rejected argument that by breaching WA surveillance devices legislation, the agreement could not be approved; FWC held s. 192, FW Act only precludes approval of agreements inconsistent with Federal (not State) laws). See also *CPSU v. VicForests* [2011] FWA 3079 (FWC conciliation assisted parties to reach agreement on implementation of GPS-based surveillance).
99. CCH, *supra* n. 44, at [20-310] and [20-400]–[20-430]. Under the NSW legislation, 'overt' surveillance is permitted subject to compliance with the statute's requirements, while 'covert' surveillance usually requires a warrant to be issued by a magistrate (on the basis that unlawful activity is suspected).
100. Cusack, *supra* n. 89.

[D] Drug and Alcohol Testing

Testing of employees for the presence of drugs, alcohol or other substances that have a capacity to impair performance is another fairly widespread practice in Australia, usually justified on the basis of the employers' obligations under WHS legislation.[101] The legality of such testing is reasonably clear: although there is no statutory basis for it (apart from mandatory testing requirements in certain industries, e.g. public transport, mining), at common law employers can direct employees to undergo a drug or alcohol test as long as the request is reasonable.[102] Further, industrial tribunals tend to support the prerogative of management to implement testing as part of a workplace drug and alcohol policy with appropriate safeguards of employees' interests.[103] The terms of any applicable employment contract, modern award or enterprise agreement may also be relevant to whether an employer has a right to insist on drug or alcohol testing.[104] In numerous decisions, workers have been found to have been lawfully dismissed for failing a drug/alcohol test; and/or for dishonesty associated with drug/alcohol-related activity or the testing itself.[105]

It was noted in 2012 that: 'Typically [drug and alcohol testing] can occur through the taking of blood, urine, saliva, and hair samples as well as breath tests.'[106] Recently, however, there has been some controversy surrounding the testing of oral fluid, with the National Association of Testing Authorities, Australia withdrawing accreditation for on-site drug testing of oral fluid due to questions over its reliability as a basis for determining cannabis use (among other factors).[107] Despite this, the FWC has since declined an employer's request to allow it to conduct urine testing (rather than saliva-based swab tests).[108]

---

101. See generally Jim Nolan, *Employee Privacy in the Electronic Workplace Pt 2: Drug Testing, Out of Hours Conduct and References*, Priv. L. & Policy Reporter 61 (2000); Peter Holland, Amanda Pyman & Julian Teicher, *Negotiating the Contested Terrain of Drug Testing in the Australian Workplace*, 47 J. Indus. Rel. 326 (2005); Creighton & Stewart, *supra* n. 58, at 438. Mandatory drug and alcohol testing on construction sites is soon likely to become a requirement for tenderers seeking to obtain Victorian government-funded building work: see *Victorian Building Workers Face Drug and Alcohol Testing Plus Monitoring*, Workplace Express (6 February 2014).
102. *Australian Federated Union of Locomotive Engineers v. State Rail Authority of New South Wales* (1984) 295 CAR 188 at 188–193; *Anderson v. Sullivan* (1997) 148 CLR 633 at 647–648; discussed in CCH, *supra* n. 44, at [20-460].
103. CCH, *supra* n. 44, at [20-460] including reference to *Caltex Australia Limited v. Australian Institute of Marine and Power Engineers, Sydney Branch; Australian Workers Union* [2009] FWA 424.
104. CCH, *supra* n. 44, at [20-460].
105. See e.g. *McCarthy v. Woolstar Pty Ltd* [2014] FWC 1186 (dismissal of forklift driver upheld following laboratory test for cannabis use); *Pitts v. AGC Industries Pty Ltd* [2013] FWCFB 9196 (employee failed to meet drug test deadline because provided unsuitable sample, diluted by drinking two bottles of water immediately prior to test); *Vaughan v. Anglo Coal (Drayton Management) Pty Ltd* [2013] FWC 10101 (employee dishonestly claimed had taken cold and flu tablets, rather than methamphetamines, prior to test).
106. CCH, *supra* n. 44, at [20-460].
107. Ashurst Australia, *To Pee or Not to Pee? Drug Testing Is the Question Again*, Employment Alert (28 October 2013).
108. *Endeavour Energy* [2014] FWC 198, reported in *FWC Rejects Bid for On-Site Urine Drug-Testing Regime*, Workplace Express (17 January 2014); see also *Maritime Union of Australia v. DP*

It is likely that the employee records exemption from the *Privacy Act* would apply to information about an employee acquired through drug or alcohol testing, as this information would clearly be relevant to the employee's employment.[109] However, any external agencies involved in the testing would be subject to the requirements of the *Privacy Act*.[110]

[E] Dismissal of Employees for Social Media-Related Misconduct

As mentioned a number of times in this chapter, employee use of social media has become a major employment issue in Australia recently,[111] with a rise since 2010 in unfair dismissal cases involving alleged serious misconduct by employees for social media activity.[112] The general trend in these decisions has been to uphold the dismissal where the employee's social media posts (even if 'private') are highly offensive or derogatory towards the employer and have (or could) cause serious harm to the business. On the other hand, other factors – such as an employee's inexperience with forums like Facebook, and length of service with an employer – can result in a finding of unfair dismissal in these cases. Space does not permit a complete discussion of this case law.[113] However, some of the more interesting and significant decisions include the following.

[1] Employee's Conduct Justified Dismissal

- *O'Keefe v. Williams Muir's Pty Ltd* [2011] FWA 5311: employee's offensive comments on Facebook about pay discrepancies found to provide grounds for summary dismissal; although privacy settings set to maximum and employer not named, comments were seen by several co-workers and considered to be threatening in nature.
- *Margelis v. Alfred Health* [2012] FWA 5390: IT administrator's dismissal for reasons including highly offensive online conversation with co-worker, upheld; such conversations using work computer found to be inherently non-private.

World Brisbane Pty Ltd and Others [2014] FWC 1523, stayed in [2014] FWC 2404 pending an appeal before a Full Bench of the FWC (not concluded at the time of writing).

109. *Ibid.*; although employers should keep such information confidential, see Creighton and Stewart, *supra* n. 58, at 438.
110. CCH, *supra* n. 44, at [20-460].
111. On privacy issues relating to the use of social media generally see Margaret Jackson & Marita Shelly, *Electronic Information and the Law* ch. 9(Thomson Reuters Lawbook Co. 2012).
112. Employees covered by the FW Act may bring a claim for unfair dismissal under Part 3-2 of the legislation (unless they fall within one of the exclusions from eligibility to bring a claim); see further Creighton and Stewart, *supra* n. 58, at 632–656.
113. See e.g. Thornthwaite, *supra* n. 4; Louise Floyd & Max Spry, *Four Burgeoning IR Issues for 2013: Adverse Action; Social Media & Workplace Policy; Trade Union Regulation (after the HSU Affair); and the QANTAS Aftermath* (2013) 37 Australian Bar Rev. 153, 160–164; Bland & Waterhouse, *supra* n. 3.

– *Little v. Credit Corp Group Limited* [2013] FWC 9642: employee's dismissal for grossly offensive Facebook comments regarding sexual harassment of a co-worker,[114] and criticism of employer's key stakeholder, upheld; employee's claim that did not know how Facebook worked dismissed as highly implausible (young person, frequent user of Facebook). The social media posts were likely to be deeply offensive and damaging to employer's business.
– *Banerji v. Bowles* [2013] FCCA 1052:[115] Federal Circuit Court refused injunction preventing dismissal of public servant in Department of Immigration and Citizenship, who anonymously made comments on Twitter criticising Federal Government's policies on immigration detention. Dismissal found to be consistent with Australian Public Service Code of Conduct, including limits on unofficial public comment. Implied freedom of political expression under *Australian Constitution* does not extend to provide unfettered rights of expression, and did not extend to comments 'tweeted' by employee to her 700 followers.[116]

[2] Employee Succeeded in Unfair Dismissal Claim

– *Fitzgerald v. Dianna Smith t/a Escape Hair Design* [2010] FWA 7358, upheld on appeal [2011] FWAFB 1422: employee's Facebook post (read by 'friends' including some of employer's clients), complaining of warning issued by employer and failure to provide holiday pay,[117] found to be a 'foolish and silly' outburst but not so detrimental to employer's business as to justify dismissal.
– *Wilkinson-Reed v. Launtoy Pty Ltd* [2014] FWC 644: held, employee unfairly dismissed by principal of car sales business for making critical comments about him in private Facebook chat with the principal's wife. Company's social media policy did not extend to preclude such communications, which were in the manner of a private email.
– *Linfox Australia Pty Ltd v. Stutsel* [2012] FWAFB 7097, upheld by Full Federal Court in *Linfox Australia Pty Ltd v. Fair Work Commission* [2013] FCAFC 157: employee's dismissal for making racially derogatory and sexually offensive comments about managers on Facebook, held to be harsh, unjust and unreasonable; employee reinstated. Relevant factors included employee's lengthy service and good employment record; limited understanding of how Facebook worked (e.g. that comments could be disseminated more broadly than just his

114. See also Paul O'Halloran, *Cyber-Sexual Harassment at Work*, Internet L. Bull. 123 (October 2012).
115. This was in fact a general protections/adverse action claim under Part 3-1 of the FW Act, rather than an unfair dismissal claim; on Part 3-1 see further Creighton and Stewart, *supra* n. 58, at 557–574.
116. See Stephen Price & Allison Grant, *Social Media: Private Life and Work Life Collides Again*, Corrs Chambers Westgarth (9 September 2013).
117. Her exact words were: 'Xmas "bonus" along side a job warning, followed by no holiday pay!!! Whoooooo! The Hairdressing Industry rocks man!!! AWSOME!!! [sic]'.

170 'friends'); fact that conduct occurred outside work hours; and that employee did not intend comments to be seen by managers. Also important was the company's failure to have a policy on employees' use of social media.

In a number of these decisions, the FWC has made some general comments about employee social media use that will no doubt be instructive in future cases. For example, in *Fitzgerald v. Dianna Smith t/a Escape Hair Design* [2010] FWA 7358 it was stated that ([50]-[51]):

> Postings on Facebook and the general use of social networking sites by individuals to display their displeasure with their employer or a co-worker are becoming more common. What might previously have been a grumble about their employer over a coffee or drinks with friends has turned into a posting on a website that, in some cases, may be seen by an unlimited number of people. Posting comments about an employer on a website (Facebook) that can be seen by an uncontrollable number of people is no longer a private matter but a public comment.
>
> It is well accepted that behaviour outside working hours may have an impact on employment 'to the extent that it can be said to breach an express term of [an employee's] contract of employment'. (Rose v. Telstra, AIRC Print Q9292 (4 December 1998))[118]

And despite the lenient approach adopted in *Linfox Australia Pty Ltd v. Stutsel* [2012] FWAFB 7097, it was also stated that ([26]):

> In the present case, the series of Facebook conversations in which the comments were made were described by the Commissioner as having the flavour of a conversation in a pub or cafe, although conducted in electronic form. We do not agree altogether with this characterisation of the comments. The fact that the conversations were conducted in electronic form and on Facebook gave the comments a different characteristic and a potentially wider circulation than a pub discussion. Even if the comments were only accessible by the 170 Facebook "friends" of the Applicant, this was a wide audience and one which included employees of the Company. Further the nature of Facebook (and other such electronic communication on the internet) means that the comments might easily be forwarded on to others, widening the audience for their publication. Unlike conversations in a pub or cafe, the Facebook conversations leave a permanent written record of statements and comments made by the participants, which can be read at any time into the future until they are taken down by the page owner. Employees should therefore exercise considerable care in using social networking sites in making comments or conducting conversations about their managers and fellow employees.[119]

Thornthwaite concludes, from her summary of the case law, that: '… for employees to comply with their implied contractual duties they cannot safely communicate about

118. See also *When Work and Out-of-Hours Conduct Clash: Lessons from the Case Law*, Workplace Express (15 March 2013); and Thornthwaite, *supra* n. 4, at 170: 'An employer … must be able to show a sufficient, requisite connection between the employee's off-duty conduct and the employment relationship legitimately to terminate them or otherwise adversely affect their employment on the basis of off-duty conduct.'
119. See also *Social Media Ignorance Less Likely to Get Employees Off the Hook: VECCI Director*, Workplace Express (10 February 2014).

their work lives in [social media] forums. Social media does appear to have had the effect that employees are never entirely off-duty.'[120]

Finally, many Australian employers have adopted social media policies and require employees to undertake social media training.[121] In one recent case, an employee's refusal to participate in such training was found to provide lawful grounds for dismissal for serious misconduct.[122] More controversially, the Department of Prime Minister and Cabinet introduced a very restrictive social media policy in April 2014, prohibiting employees from (among other things) engaging in harsh or extreme criticism of the government or its policies; and requiring employees to report social media breaches by their colleagues to the Department.[123]

[F] Employers' Obligations to Maintain Employee Records under the Fair Work Act

Employers covered by the *FW Act* are *required* to maintain various employee records, to ensure that employees receive their correct pay and entitlements under that legislation and any modern awards or enterprise agreements that apply to their employment.[124] Civil penalties of up to AUD 2,550 apply to breaches of these obligations.

Known colloquially as 'time and wages records', these employee records must be kept for seven years in the form prescribed by the *Fair Work Regulations 2009* (Cth) (*FW Regulations*), and must include the following information:[125]

- names of employer and employee;
- type of employment (full-time, part-time, casual, etc.);
- employee's date of commencement;
- Australian Business Number of employer (where applicable);
- employee's rate of remuneration (gross and net pay, any deductions); bonuses; loadings; penalty rates; other monetary allowances;
- overtime hours worked; hours of work for casual/irregular part-time employees;
- leave taken by employee (annual leave, personal/carer's leave, etc.); balance of leave entitlements;
- information relating to superannuation contributions made by employer on behalf of employee;

120. Thornthwaite, *supra* n. 4, at 184.
121. See e.g. *Twitter Ban at Work Counterproductive: Telstra*, Workplace Express (20 April 2009); *Unions Concerns Trigger Commbank Rethink on Social Media*, Workplace Express (7 February 2011). Increasingly, enterprise agreements are including workplace social media restrictions: see *Agreements Outlaw Facebook at Work and Seek to Limit After-Hours Use*, Workplace Express (7 December 2012).
122. *Pearson v. Linfox Australia Pty Ltd* [2014] FWC 446; upheld on appeal [2014] FWCFB 1870.
123. *Social Media Policy of the Department of the Prime Minister and Cabinet*, 8 April 2014; this policy is in part a direct response to *Banerji v. Bowles* [2013] FCCA 1052 (*supra*).
124. *FW Act*, s. 535(1).
125. *FW Act*, s. 535(2); *FW Regulations*, Chapter 3, Part 3-6, regulations 3.31–3.41.

– details of termination of employment (e.g. whether by consent, by notice, summarily or other form of dismissal).

An employee is entitled to inspect and copy his/her employment record, upon request to the employer (former employees may also exercise this right).[126] Employee records may also be accessed by the Fair Work Ombudsman (the Federal agency responsible for enforcement of minimum employment standards),[127] or a trade union representing an employee whose employment rights may have been infringed.[128] Employers must correct any error in an employee record as soon as the employer becomes aware of the error (e.g. once it is drawn to the employer's attention by an employee or union).[129] In effect, these provisions give employees some of the rights they would have under the NPPs if the employee records exemption under the *Privacy Act* did not apply.[130]

§1.05 PERSONAL INFORMATION AND PRIVACY PROTECTION AFTER THE EMPLOYMENT RELATIONS

As indicated earlier in this paper, the employee records exemption from the *Privacy Act* applies not only to current but also former employment relationships. As a result, any personal information relating to a former employee held within an employee record could be provided by the former employer to another prospective employer – e.g. information about the employee's performance, training, (mis)conduct, any disciplinary action, and reasons for termination.[131] However, such information *would* be subject to the *Privacy Act* in the hands of the prospective employer. Commonly, information about a former employee will be provided in a reference. Although not obliged to provide a reference for a former employee, employers must be careful when they do so not to include any misleading or defamatory material.[132]

Another post-employment issue that has arisen in a number of recent cases is the use by former employees of social media sites such as LinkedIn to solicit business from clients of their former employer (alternatively, this might occur while an employee is still employed but making moves to start out on their own or join another business). Such conduct is likely to breach an employee's implied contractual obligations, or express restraint clauses/restrictive covenants, not to engage in competition with a former employer; not to solicit its customers or staff; and not to misuse the former employer's confidential information.[133]

126. *FW Regulations*, Chapter 3, Part 3-6, regulations 3.42–3.43.
127. *FW Act*, ss 708, 712, 714; *FW Regulations*, Chapter 3, Part 3-6, regulation 3.31 (records must be kept 'in a form that is readily accessible to an inspector').
128. *FW Act*, ss 482–483.
129. *FW Regulations*, Chapter 3, Part 3-6, regulation 3.44.
130. CCH, *supra* n. 44, at [20-200].
131. Carolyn Sappideen, Paul O'Grady, Joellen Riley and Geoff Warburton, *Macken's Law of Employment*, Thomson Reuters Lawbook Co, Sydney, 7th edition, 2011, 202–203.
132. *Ibid*., 202–206.
133. See e.g. *Pedley v. IPMS Pty Ltd t/a peckvonhartel* [2013] FWC 4282; Chris McLeod & James Neil, *Employees, Social Media and Confidential Information: Uneasy Bedfellows*, Internet L. Bull. 134

§1.06 CONCLUSION

In 2000, the Office of the Australian Information Commissioner stated that: 'It is clear that most staff do not expect to completely sacrifice their privacy while at work.'[134] This sentiment is reflected in data from a 2004 survey commissioned by the Federal Privacy Commissioner, showing that 34% of respondents felt employers should not have any access to employees' work emails; 35% objected to the use of surveillance equipment in the workplace; and 59% opposed random drug testing.[135]

However, as this chapter has shown, the actual extent of privacy protection afforded to Australians in the workplace is limited – and inconsistent in different parts of the country. Ironically, workers have more protection of their personal information *before* commencing employment, given that the employee records exemption from the *Privacy Act* does not apply during the recruitment process. Prospective employees are also the subject of discrimination law protections, and safeguards in relation to health screening and the use of information relating to criminal records.

Once in a job, personal information relating to an employee's employment is not covered by the protections provided under the *Privacy Act*. The employee's use of email and internet in the workplace (or outside) may be the subject of monitoring and surveillance, as may his/her phone calls and even movements (through GPS tracking) – with differing levels of safeguards under Federal, State and Territory laws. There is a fairly permissive approach to drug and alcohol testing in Australia, and increasingly the social media activities of employees are being called into question in unfair dismissal cases.

Given the overhaul of the *Privacy Act* through the 2012 amendments, further major legislative change in this area is unlikely. Nor does there seem to be any impetus for uniform national regulation of workplace surveillance. It can be expected, then, that Australian law will continue to provide employees with only 'a thin wall of privacy protection, with gaps and cracks' for some time to come.

(October 2013). On the law relating to the implied duty of fidelity, and the enforceability of express restraint clauses, see Creighton and Stewart, *supra* n. 58, at 413–416, 423–428.

134. Australian Government, Office of the Australian Information Commissioner, *supra* n. 16.

135. Roy Morgan Research, *Community Attitudes towards Privacy 2004*, discussed in *Research on Australian Attitudes towards Privacy – Part 1*, 1:6 Priv. L. Bull. 93, 95 (2004).