DETERMINING CURRENT JUDICIAL TRENDS IN DEFINING PARAMETERS OF PRIVACY AT THE WORKPLACE IN RELATION TO SOCIAL MEDIA USE BY EMPLOYEES — AN AUSTRALIAN CONTEXT

AJANTHA THINKARAN

Lawyer Admitted to Practice in the Supreme Court of Western Australia and High Court of Australia

Bachelor of Laws with Honours (University of London)

This thesis is presented for the degree of Master in Laws by Research of Murdoch University

February 2018

Student number: 31696343

Declaration

I declare that this thesis is my own account of my research and contains as its main content work which has not previously been submitted for a degree at any tertiary education institution.

This Thesis was submitted for professional editing by Capstone Editing Pty Ltd of 15 Moore Street, Cannberra, ACT 2601 and that the editing and proof-reading by professional editors complies with the approved standards as set out on the GR website.

……

(Ajantha Thinakaran)

Abstract

The legal issues that relate to the realm of privacy, social media communication and technology are ever growing. In Australia, over the past five years or so, there have been a series of dismissals resulting from the use of personal social media communications by employees. One area of dismissals is employers terminating employees for complaining about their colleagues in the employee's personal social media space. Another example is employees discussing workplace processes and procedures in the employee's personal social media space leading to alleged disclosures of confidential information.

Several questions concern these dismissals. These include determining how courts view individual employees' personal social media sites, either as a private space or a public space. This appears to provide a basis for how courts view employer regulation of employees' social media interaction, regardless of whether such interaction relates directly, or is incidental, to workplace activities. When employer control is permitted, judicial decisions are also relevant in understanding the extent to which courts may permit employers to exercise such control.

As this area is still new, much of the body of cases referred to lie in Fair Work Commission decisions. The above is researched under the overarching theme of identifying current judicial trends in determining parameters of privacy in the workplace in relation to social media use by employees. Judicial determination of these issues is important, as legislation still lags behind the massive and rapid technological advances in social media communication. In Australia, the courts are still the primary influencers and protectors of privacy as a human right. Judicial

clarification of privacy, employer control over employees and employee dismissals within the existing workplace legislation is important for both employers and employees alike.

Contents

Acknowledgments

This Master's Thesis would not have been possible without the support, encouragement and patience of my supervisors, in particular Dr Steve Shaw who wielded the whip and served ice cream in equal measure, Dr Peter Waring who believed in me when no else did, my colleagues at Murdoch Singapore, Ms Natalie Van der Waarden and Ms Anne Clear, Dr Julia Hobson, and my family in particular my siblings Dhinesh Thinakaran and Brindha Dyer and uncles, aunties, and cousins. I acknowledge the services of Capstone Editing for the final edit.

This Thesis is dedicated to my parents, Uma and Thinakaran, and my Guru, Swami Shantanand Saraswathy.

Part 1: Literature Review

1.1. Introduction

Contemporary or digital social media, most often described as social media (SMedia), has fundamentally transformed communication.[1] Many individuals use their SMedia accounts as their primary mode of social interaction.[2] Dedicated SMedia platforms such as Facebook, Yahoo and Google incorporate both SMedia and general news media. By 30 June 2017, Facebook had an average of 1.32 billion daily active users and 2.01 billion monthly active users worldwide.[3] In Australia, the use of SMedia has increased significantly in recent years.[4] Instagram is one of fastest growing SMedia sites in terms of user numbers.[5] In the last year, Instagram users increased from 1.6 million to 5 million.[6] The majority (66 per cent) of the Australian population use SMedia outside work as a place for social interaction.[7] These statistics show the sheer volume of SMedia users and indicate that the majority of online activity is predominantly social interaction of some form or another. The statistics also show the prevalence of SMedia as a significant mode of social

---

[1] Stephanie Vass, 'The Anti-Social Network? Unfair Dismissal and Facebook' (2011) 2(4) *Workplace Review* 139.
2 Pauline Rappaport, 'Social Media Policies and Unfair Dismissal' (2013) 18(2) *Media and Arts Law Review* 75.
3 Facebook, *Company Info — Stats* (2017) Facebook Newsroom <https://newsroom.fb.com/company-info/>.
[4] Sally Wood, 'Statistics for Social Media Usage in Australia: What They Mean for Your Online Marketing Efforts', *Marketing.com.au*, 3 July 2015 <https://marketing.com.au/statistics-for-social-media-usage-in-australia/>.
[5] Ibid.
[6] Ibid.
[7] Australian Bureau of Statistics, *8146.0 — Household Use of Information Technology, Australia, 2012–13: Patterns of Home Internet Use* (25 February 2014) <http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/8A12E6E0D07D36A0CA257C89000E3FB7>.

interaction — one that, until recently, did not exist. Previously, social interaction would have occurred face-to-face, by telephone or through traditional postal services. From a sociological context, SMedia is sometimes regarded as an impersonal mode of communication.[8] Despite high interaction between users, there is no human eye, touch or voice contact. Whether this affects users of SMedia in the workplace and whether it is a legally relevant issue will be discussed in the definition of SMedia later in this paper.

By February 2011, 49 per cent of personal SMedia use was initiated from the workplace.[9] The increased use of SMedia in the workplace as a primary mode of communication, both within the employment context and as a form of social interaction, has created uncertainty in relation to balancing individual privacy and employer control.[10] Some of the questions that arise in SMedia use at work are based on the right to privacy. Other questions focus on determining what rights employers have to oversee their employees' SMedia use.

It is becoming increasingly common for employees to lose their jobs because of some aspect of their personal SMedia use.[11] This has led to allegations of unfair dismissal by the affected employees.[12] Conversely, employers have their own

---

[8] Robin Dunbar, 'You've Got to Have (150) Friends', *New York Times* (online), 25 December 2010 <http://www.nytimes.com/2010/12/26/opinion/26dunbar.html>. Robin Dunbar is a professor of evolutionary anthropology at Oxford University. See generally, Robin Dunbar, *How Many Friends Does One Person Need? Dunbar's Number and Other Evolutionary Quirks* (Harvard University Press, 2010).

[9] Australian Bureau of Statistics, *8146.0 — Household Use of Information Technology, Australia, 2010–11: Personal Internet Use* (15 December 2011) <http://www.abs.gov.au/ausstats/abs@.nsf/0/D11394A54F8B9ED1CA25796600152C62>.

[10] Vass, above n 1.

[11] Andrew Carney, 'Unfair Dismissal Relating to the Use of Social Media — An Analysis of Case History' (2014) 12(1) *Canberra Law Review* 144.

[12] See, eg, *Pearson v Linfox Australia Pty Ltd* [2014] FWC 446 [46]. In this case, an employee was dismissed for reasons including his failure to sign the company's social media policy. The employee had argued that the social media policy affected his life 'outside' work hours. His allegation of unfair

perspective and priorities. These priorities include safeguarding their brand reputation,[13] keeping their corporate secrets safe[14] and maintaining the internal harmony of the workplace environment (eg, preventing the harassment of other employees).[15] The body of rigorous academic literature in this area is still 'very much in its infancy'.[16] For that reason, the literature that forms the basis of this thesis is sourced not only from case law, legislation and academic discourse, but also from discussions on SMedia sites. These will include, for example, practitioner blogs and commentary in legal firm law updates and reviews, Twitter feeds, news reports, academic books and other generalist publications.[17] Two queries or issues emerge from early research into this area. First, why is there a lack of rigorous academic research in this specific area of employment? Second, what areas involving employment law and SMedia use are the focus of academic research? This thesis will address and attempt to answer these two questions.

1.2. The Gaps in Research

The first question this thesis addresses is: why is there a lack of rigorous academic research in this specific area of employment?

---

dismissal did not succeed. In relation to this specific ground, the court opined that the company was entitled to protect its reputation and that the SMedia policy was a means of placing parameters of acceptable SMedia communication. The court further indicated that social media can no longer be considered a private realm of communication.

[13] See *Mayberry v Kijani Investments Pty Ltd ATF The Dawe Investments Trust Subway Wallsend* [2011] FWA 3496.

[14] See Press Trust of India, 'Corporate Business Secrets Getting Leaked on Social Media Websites', *Economic Times* (online), 21 November 2011 <https://economictimes.indiatimes.com/tech/internet/corporate-business-secrets-getting-leaked-on-social-media-websites/articleshow/10816341.cms>.

[15] See *Stutsel v Linfox Australia Pty Ltd* [2011] FWA 8444.

[16] Louise Thornthwaite, 'Social Media, Unfair Dismissal, and the Regulation of Employees' Conduct Outside Work' (2013) 26 *Australian Journal of Labour Law* 164.

[17] Ibid.

Briefly, research in the employment sector is mainly focused on other areas of privacy. The freedoms and restrictions with which employees use SMedia sites have been outside the scope of this research. The two primary areas that are researched are data privacy[18] and cybersecurity.[19] These areas overarch and branch into other areas of law that will be examined below.

1.2.1. Data privacy

Before beginning a discussion of what data privacy is, a definition of *data* must be considered. One classification of data is 'informational data', meaning personal information relating to individuals that SMedia companies such as Facebook collect through their platforms.[20] Another description of data is 'any information relating to an identified or identifiable individual'.[21] SMedia companies collect the data when individuals access websites and provide this to advertisers to aid in predicting target markets.[22] Issues relating to privacy arise when individual consumers have not authorised the collection and use of their personal information or personal preferences.[23]

---

[18] A Michael Froomkin, 'The Death of Privacy?' (2000) 52(5) *Stanford Law Review* 1461.
[19] Michael Pattison, 'Australia' in Alan Charles Raul (ed), *Privacy, Data Protection and Cybersecurity Law Review* (Law Business Research Ltd, 2nd ed, 2015) 38.
[20] Ibid.
[21] *Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data* [2001] OJ L 8/1, art 2(a). See also European Union Agency for Fundamental Rights, *Data Protection* (2017) European Union Agency for Fundamental Rights <http://fra.europa.eu/en/data-protection>.
[22] Julia Angwin, 'The Web's New Gold Mine: Your Secrets', *The Wall Street Journal* (online), 30 July 2010 <https://www.wsj.com/articles/SB10001424052748703940904575395073512989404>; Aleksandra Korolova, 'Privacy Violations Using Microtargeted Ads: A Case Study' (2011) 3(1) *Journal of Privacy and Confidentiality* 27.
[23] Alex Hern, 'Windows 10: Microsoft Under Attack Over Privacy', *The Guardian* (online) 1 August 2015 <https://www.theguardian.com/technology/2015/jul/31/windows-10-microsoft-faces-criticism-over-privacy-default-settings>.

One contemporary issue related to the collection of unauthorised data and data privacy is the European Union's collective legal assault against the unauthorised collection of personal information of citizens belonging to European Union (EU) member states by corporations and entities incorporated in the United States (US). This assault is conducted through legal actions in the European Court of Justice and European Court of Human Rights and is spearheaded by EU member states. It is an attack against the actions of SMedia giants Facebook and Google in relation to the collection, use and transfer of data belonging to individuals residing in EU member states.[24] One example is *Maximillian Schrems v Data Protection Commissioner* (Court of Justice of the European Union, C-362/14, 6 October 2015).[25] This matter involved an Austrian Facebook user who had all or some of his Facebook account data moved between servers to be processed. The data was moved from Facebook's subsidiary in Ireland to its servers in the US. This case is discussed further below. These actions have had a socio-political effect on privacy laws and treaty arrangements regarding the transfer of data between the US and the EU. This has led to the *Safe Harbor Privacy Principles*[26] (*SHPPs*), a joint agreement between the EU and the US, being rendered defunct by the European Union Court of Justice.[27]

The *SHPPs* were developed to facilitate the transfer of personal information belonging to individuals from the EU to the US. The *SHPPs* were meant to ensure

[24] Court of Justice of the European Union, 'The Court of Justice Declares that the Commission's US Safe Harbour Decision is Invalid' (Press Release, 117/15, 6 October 2015).
[25] *Maximillian Schrems v Data Protection Commissioner* (Court of Justice of the European Union, C-362/14, 6 October 2015).
[26] PrivacyTrust*, PrivacyTrust Safe Harbor Program* <https://www.privacytrust.com/safeharbor/>.
[27] Hern, above n 23.

that any data transferred would be in accordance with the requirements of the EU's *Data Protection Directive [1995] OJ L 281/31*.[28] The *SHPPs* were given legal recognition via the European Commission's adoption of the same.[29] The *SHPPs* were only applicable to entities incorporated in the US and adherence to the *SHPPs* was not mandatory. The *SHPPs* merely required that US-based entities register with the US Department of Commerce. Once registered, the entities were deemed to be compliant with EU data protection legislation.[30] Compliance was based on self-certification and self-assessment by the entities that were then deemed to be regulated, if required, by the intervention of the US Department of Commerce.[31] This thesis submits that the idea was that as a signatory of the *SHPPs* the US and its corresponding departments would be compliant. *Maximillian Schrems v Data Protection Commissioner*[32] highlighted the weaknesses in the *SHPPs*. It appears that the main flaw was that once the data had been transferred it was subject to the laws of the US, meaning that the data could be scrutinised by security agencies in the US or be used in a way that was not compatible with the EU's concepts of individual privacy.[33]

---

[28] *Council Directive 95/46/EC of the European Parliament and of the Council of the 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* [1995] OJ L 281/31.
[29] European Commission, *Communication from the Commission to the European Parliament and the Council: Rebuilding Trust in EU–US Data Flows* (27 November 2013) <http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf>.
[30] Ibid.
[31] *Maximillian Schrems v Data Protection Commissioner* (Court of Justice of the European Union, C-362/14, 6 October 2015) [14] [17].
[32] *Maximillian Schrems v Data Protection Commissioner* (Court of Justice of the European Union, C-362/14, 6 October 2015).
[33] Ibid [53].

The judgment in *Maximillian Schrems v Data Protection Commissioner*[34] highlights a fundamental difference between European and American concepts of privacy. European law seeks to protect individual privacy with less regulatory interception.[35] Conversely, the US has, especially since the September 11 terrorist attacks, encroached individual privacies through increased surreptitious, albeit lawful, surveillance of individuals.[36] This difference, and the effect it may have on a comprehensive and coherent data privacy regime (particularly regarding the US-proposed Privacy Shield)[37] will undoubtedly be the subject of much scrutiny and research. The management of how data is currently transferred from EU to the US will have an overarching effect within the context of the international legal framework that has been set up to manage the privacy and control of data transfer from one country to another. While this is a fascinating area of research, it is not the subject matter of this thesis.

In relation to current data privacy frameworks, the judgment in *Maximillian Schrems v Data Protection Commissioner* has the potential to render unlawful any transfer of personal data from the EU to the US. The SMedia giants involved in the case, Facebook and Google, both continue to be under intense legal scrutiny in Europe

---

[34] *Maximillian Schrems v Data Protection Commissioner* (Court of Justice of the European Union, C-362/14, 6 October 2015).
[35] Ibid.
[36] Marguerite Rigoglioso, 'Civil Liberties and the Law in the Era of Surveillance' (2014) 49(91) *Stanford Lawyer*, Cover Story.
[37] Following the above decision in *Maximillian Schrems v Data Protection Commissioner* (Court of Justice of the European Union, C-362/14, 6 October 2015), the two nations agreed to establish a new (and as yet unratified by the European Union) *European Union–United States of America Privacy Shield* to replace the *Safe Harbor Framework*. See Federal Trade Commission, *Privacy Enforcement and Safe Harbor: Comments of FTC Staff to European Commission Review of the US–EU Safe Harbor Framework* (12 November 2013) <https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-enforcement-safe-harbor-comments-ftc-staff-european-commission-review-u.s.eu-safe-harbor-framework/131112europeancommissionsafeharbor.pdf>.

for unlawfully collecting and transferring the information of private individuals in various European countries such as France[38] and Belgium.[39]

There is a large body of literature that focuses on this area of privacy. Some fall within the purview of employer–employee relationships and will be discussed later in this thesis. Other areas of research into data privacy include data collected by various (non-media) government and private agencies such as data relating to health and education. However, the principles of law related to these are established law in most developed countries and such data has varying degrees of privacy protection.

In Australia, the *Australian Privacy Principles* (*APPs*) mandate that personal information should be safeguarded.[40] The 13 principles of *APPs* are set out in Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) that amends the *Privacy Act 1988* (Cth) (the *Act*). As part of an effort to protect personal information, the *APPs* set out clear guidelines as to when and how personal information can be collected or stored by any entity seeking to collect such information. The informed consent to authorise collection, storage and disclosure of personal information of the person whose details are being collected remains at the forefront of this legislation.[41] However, there are separate guidelines as to the use of an individual's information without consent.[42] The use of collected data is limited, whether it be authorised by an individual or not. In the absence of any specific

[38] David Meyer, 'Here's Why France's Demands Could Hammer Facebook's Business Model', *Fortune* (9 February 2016) <http://fortune.com/2016/02/09/france-facebook-advertising/>.
[39] David Meyer, 'Belgian Police Say Facebook Reactions Could Be Dangerous', *Time* (online), 12 May 2016 <http://time.com/4327641/belgian-police-facebook-reactions-dangerous>.
[40] Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) amends the *Privacy Act 1988* (Cth).
[41] Ibid.
[42] See ss 95, 95A and 95AA of the *Privacy Act 1988* (Cth).

authorisation to the contrary, such data is only used after de-identifying it from the individual.[43] This signifies that a shift is occurring within the Australian government, specifically the Office of the Australian Information Commissioner (OAIC).[44]

The OAIC is responsible for determining the scope and ambit of the *APPs*. Its guidelines demonstrate a move towards the ideal of open access to the government-held private information of individuals.[45] A speech by the Acting Australian Information Commissioner, Timothy Pilgrim, indicates that, in line with the above approach, the portions of personal information held by government agencies may be declared 'open access by default' and not be protected by the *Act*.[46] The rationale for this is that personal information collected and stored by government agencies presents 'an immensely valuable data resource for policy, planning, research and innovation — ultimately providing better services to Australian businesses and communities'.[47] This may well herald a new approach to data privacy that may directly or indirectly effect employee data collected by the employer. This thesis submits that one potential effect on employee data is a new and possibly analogous approach by the courts and other bodies in determining how personal information is perceived. For example, in deciding whether such information is classified as being private and consequently protected by the *APPs*, courts may follow the Information Commissioner's view that there are public policy reasons to reduce privacy

[43] *Privacy Act 1988* (Cth), Part III — Information Privacy in conjunction with the *APPs* (particularly Policy 1) lays down the circumstances in which personal information of an individual may be disclosed and when it may not be disclosed.
[44] Previously the Office of the Australian Privacy Commissioner.
[45] Timothy Pilgrim, 'The Value of Public Sector Information' (Speech delivered at the AGS FOI and Privacy Forum, Canberra, 4 May 2016) <https://www.oaic.gov.au/media-and-speeches/speeches/the-value-of-public-sector-information>. Note, this speech does not make a distinction between health data and other data.
[46] Ibid.
[47] Ibid.

restrictions.[48] This thesis submits that such an approach by the courts may even lead to amendments in related workplace legislation with regards to privacy.

A different model of consent to disclosure suggested by a cohort of medical data researchers is the Dynamic Consent Model.[49] This model allows for patients to retain some degree of control over their personal information and how it is used.[50] It proposes that a patient electronically control their consent with reference to the transmission and use of their own data over time. The model rests on the premise that by so doing, public trust will be maintained and this will consequently benefit medical research to leverage positively for both the patient and society as a whole.[51] The Dynamic Consent Model research considers the United Kingdom (UK) health information management system that provides the basis for the Australian system.

Another emerging research area surrounding privacy of health data examines the privacy issues around data personally collected by individuals in relation to their own bodies through purchased or free applications.[52] In this self-quantification of data, the data is collected in a device that belongs to the individual but is potentially accessible by the software provider who owns the application. People using these types of devices or applications sign a privacy agreement with the software provider.

[48] Ibid.
[49] Hawys Williams et al, 'Dynamic Consent: A Possible Solution to Improve Patient Confidence and Trust in How Electronic Patient Records Are Used in Medical Research' (2015) 3(1) *JMIR Medical Informatics* e3.
[50] Ibid.
[51] Ibid.
[52] Angela Daly, 'The Law and Ethics of 'Self-Quantified' Health Information: An Australian Perspective' (2015) 5(2) *International Data Privacy Law* 144.

Research in this area examines the information collected, how it may be stored and the purpose for which such information may be used.[53]

One example is the personal health data collected by Apple Inc through its iOS (mobile operating system) applications. One such application, or app, is the 'Health App' that comes standard with the iPhone operating system.[54] This application reassures the user that they can choose which other applications can access their personal data. However, the application automatically updates and shares health data across all of the user's various devices and uploads it onto iCloud automatically — unless the user takes the time and effort to turn off this sharing setting. The iCloud is an information storage and computing service from Apple Inc that allows information to be stored in a remote server instead of on a particular device.[55] It allows access to the stored information from any device with an internet connection.[56] As of February 2016, the service had 782 million users.[57] Once the data is uploaded onto iCloud, it is encrypted as a security measure to prevent unauthorised access from third parties and remains stored on the iCloud servers.[58] Although the data is encrypted, it remains in cyberspace and is potentially accessible to hackers.

---

[53] Ibid.
[54] Apple Inc, *A Bold Way To Look at Your Health* (2017) <https://www.apple.com/au/ios/health/>.
[55] David Price, *How to Use iCloud* (16 May 2017) Macworld <https://www.macworld.co.uk/how-to/mac-software/how-use-icloud-3659150/>.
[56] Ibid.
[57] AppleInsider Staff, *Apple Music Passes 11M Subscribers and iCloud Hits 782M Users* (12 February 2016) AppleInsider <http://appleinsider.com/articles/16/02/12/apple-music-passes-11m-subscribers-as-icloud-hits-782m-users>.
[58] Apple Inc, *iCloud Security Overview* (7 November 2017) <https://support.apple.com/en-sg/HT202303>.

The above are useful, but not exhaustive, examples that showcase some current areas of data privacy research, even though they are not specifically about employment and SMedia. It is worth noting that with regards to self-quantified health data, an individual collecting their own data may choose to share their personal information with others who utilise the same application. For example, Apple Inc provides the opportunity for Apple device users to connect and use a popular third-party sport and fitness device known as Fitbit.[59] Fitbit allows for an individual's personal fitness goals and activity to be disseminated through sharing information with others (such as friends and family) who also wear the same device or through a related Apple device such as an iPhone.[60]

An interesting issue related to the employer–employee data relationship research in this paper is the use of such data when the device is given to an employee as part of an employment package.[61] A question that arises is whether such information that may lead to inferences regarding the employee's health status is considered 'public' information and accessible by the employer for use against the employee. However, this issue is beyond the scope of this thesis.

1.2.2. Data privacy and education

The next primary area of research on data privacy is the education sector. The reasons for this are clearly articulated by Barnes and Kowalski, who state that

[59] Fitbit Inc, *How Do I Connect with Friends with Fitbit?* (2017) <https://help.fitbit.com/articles/en_US/Help_article/1858>.
[60] Ibid.
[61] Examples of workplace fitness challenges include 'Powering Employee Engagement – Investing in your employees health and well-being is really an investment in your company's bottom line> Homepage, Wellteq <wellteq.co> (Accessed 17 January 2018) and previously known as Globetrekker , <http://www.globetrekkerchallenge.com> and Homepage, Ritualize <https://ritualize.com/main/?>(Accessed 17 January 2018).

schools find it nearly impossible to manage and safeguard the mass of student data they collect.[62] This difficulty has led to almost routine data breaches of student personal information. Examples of student personal information include: student grades, financial information and disciplinary and special education records. This data is being compromised by companies who use the data without the authorisation of the individual student or who do not put in place appropriate security to prevent breaches.[63] Although these findings were made in the context of the US, the issue is equally problematic in Australia. The Department of Education and Training[64] is subject to the *Act* and thus, the *APPs* as discussed above. The Department also has in place a privacy policy developed in accordance with Australian Privacy Principle 1.[65] The privacy policy sets out the management of personal information held by the Department.[66] It details the types, methods and purposes for which personal information is collected, held or disclosed by the Department. The Department is responsible for the national policies that flow into the state levels of education encompassing all levels of education from early childhood education through to higher education, as well as aspects of the international education sector.[67]

Professor Bruce Baer Arnold from the School of Law, University of Canberra, suggests that perhaps what is lacking in this policy is clear direction concerning the methods of protection and enforcement of the existing *APPs* and the Department's

---

[62] Khaliah Barnes and Paige Kowalski, 'Role for Federal Government in Safeguarding Student Data Privacy' (2016) 16(2) *State Education Standard* 18.
[63] Ibid.
[64] Department of Education and Training, *The Department*. <https://www.education.gov.au/department>.
[65] Department of Education and Training, *Privacy Policy* (9 August 2017) <https://www.education.gov.au/privacy-policy>.
[66] Ibid.
[67] Australian Government Department of Education and Training, home page (at 14 November 2017) <https://www.education.gov.au>.

privacy policy and corresponding sanctions (if any).[68] The discussion around this area of law is closely related to the cybersecurity segment discussed below and will be addressed in that context. This paper's purpose in highlighting data breaches in the education sector is to point to the fact that it will cover an area in the research that is not yet addressed.

1.2.3. Social media use in education

Research on the use of SMedia in the field of education is fairly broad and covers a spectrum of diverse issues. Some examples of research focus include the use of SMedia as a pedagogical tool, as a form of interaction between teachers and students and as a form of peer learning or education-related interaction between students. All these areas have their respective privacy-related issues.

An analysis by Schwartz and Caduri finds that teachers utilised SMedia sites such as Facebook to manage student behaviour, enhance social learning, promote active engagement of students and encourage a degree of autonomy in student learning.[69] This analysis and the various studies provided in support of their findings are not relevant to the context of this thesis. However, the report by Schwartz and Caduri highlights that this is a focus of SMedia research in the education discipline. The privacy issues that arise in this area are more apparent in the following discussion of SMedia interaction between teachers and students.

---

[68] Bruce Baer Arnold, 'Care Don't Share: What Medvet Breach Says About Australian Privacy Laws', *The Conversation*, 8 August 2011 <http://theconversation.com/care-dont-share-what-medvet-breach-says-about-australian-privacy-laws-2594>.

[69] Baruch Schwartz and Galit Caduri, 'Novelties in the Use of Social Networks by Leading Teachers in their Classes' (2016) 102 *Computers and Education* 35.

In Israel, a 2011 survey showed that about 27 per cent of students were online friends with at least several of their teachers.[70] In April 2013, the Israel Ministry of Education issued a national ban restricting the type and mode of SMedia communication in which teachers may engage with students.[71] Hence, teachers may only communicate through distinct, professional SMedia profiles that are specially created for teacher–student interactions.[72] It appears that the Ministry's rationale for regulating and managing teacher–student online communication was to minimise the perceived 'already eroding status of teachers'.[73] SMedia interaction between students and teachers seems to have led to the blurring of professional and social 'online conduct', resulting in an unbecoming familiarity and removing teachers' authority.

1.2.4. Cybersecurity

Cybersecurity can be simplistically defined as the process of securing digital information assets from being tracked, hacked or stolen.[74] The meaning of the verb

---

[70] Christa Asterhan et al, 'Secondary School Teacher-Student Communication in Facebook: Potentials and Pitfalls' (Paper presented at Chair Conference on Instructional Technologies Research 2013: Learning in the Technological Era, Raanana, 19–20 February 2013). See also, for a discussion of social media and education, Israel Internet Association, *That's How the Internet Looks to Your Children* <https://www.isoc.org.il/sts-data/23150>.

[71] Arnon Hershkovitz and Alona Forkosh-Baruch, 'Student-Teacher Relationship in the Facebook Era: The Student Perspective' (2013) 23(1) *International Journal Continuing Engineering Education and Life-Long Learning* 35, citing Israeli Ministry of Education, *Director General Communication, Instruction 9.4-1: Education to Protectedness, to Ethic Keeping and to Appropriate and Wise Behaviour on the Web* [In Hebrew].< ttps://www.researchgate.net/publication/264821418_Student-teacher_relationship_in_the_Facebook_era_the_student_perspective> Accessed 17 January 2018

[72] Christa S C Asterhan and Hananel Rosenberg, 'The Promise, Reality and Dilemmas of Secondary School Teacher-Student Interactions in Facebook: The Teacher Perspective' (2015) 85 *Computers and Education* 134.

[73] Ibid 134.

[74] Scott Shakelford, Scott Russell and Andreas Kuehn, 'Unpacking the International Law on Cybersecurity Due Diligence: Lessons from Public and Private Sectors' (2016) 17(1) *Chicago Journal of International Law* 1, citing 'Cyber Due Diligence: Pre-Transaction Assessments Can Uncover Costly Risks' on Kroll Intelligence Center (28 January 2015) <http://blog.kroll.com/2015/cyber-due-diligence-pre-transaction-assessments-can-uncover-costly-risks/>.

'hack' has gained contemporary linguistic acceptance to include the process of accessing a computer illegally.[75] Cybersecurity is targeted to prevent the illegal access of digital information, be it personal, corporate or governmental and is important in a diverse range of areas. These include, but are not limited to, identity theft[76] (individual and corporate), national security[77] and corporate espionage.[78] Other areas that overlap with cybersecurity and the prevention or protection of the use, misuse or abuse of personal information include cyber wellness and child pornography.[79] Cyber wellness encompasses various negative aspects of online environments including cyberbullying, cyberstalking and internet addiction. Although internet addiction is not an offence[80] it can have an effect on health[81] and; therefore, may affect workplace productivity and employer–employee relationships.[82]

---

[75] Cambridge Dictionary, (online ed, 2018) 'Hack' extracted 17 January 2018 <http://dictionary.cambridge.org/us/dictionary/english/hack>.

[76] See Kenneth D Ngyuen, Heather Rosoff and Richard S John, 'The Effects of Attacker Identity and Individual User Characteristics on the Value of Information Privacy' (2016) 55 *Computers in Human Behaviour* 372.

[77] Jeroen van den Hoven et al, 'Privacy and Information Technology' *Stanford Encyclopedia of Philosophy* (online, 21 March 2016) <https://plato.stanford.edu/archives/win2014/entries/it-privacy/>. See also Danny Yadron, 'Edward Snowden: "I'm Not An Unhappy Ending" for Future Whistleblowers', *Guardian* (online), 3 April 2016 <https://www.theguardian.com/us-news/2016/apr/01/edward-snowden-whistleblower-russia-exile>.

[78]Jeroen van den Hoven et al, 'Privacy and Information Technology' *Stanford Encyclopedia of Philosophy* (online, 21 March 2016) < https://plato.stanford.edu/archives/win2014/entries/it-privacy/>. See also Alex Hern, 'Former Microsoft Employee Arrested over Windows 8 Leaks', *The Guardian (International Edition)* (online), 20 March 2014 <https://www.theguardian.com/technology/2014/mar/20/former-microsoft-employee-arrested-over-windows-8-leaks>

[79] United States Department of Justice, *Child Pornography* (25 July 2017) <https://www.justice.gov/criminal-ceos/child-pornography>, para 'Child Pornography Today'.

[80] Ajantha Comment: Although the concept of internet addiction as an offence may seem absurd, this thesis submits that the increasing emergence of studies identifying pornography, gaming and facebook use as addictions affecting the mental health of various segments of the community may prompt some form of regulatory intervention in the forseeable future.

[81] Kimberly S Young, 'Internet Addiction: The Emergence of a Clinical Disorder' (1998) 1(3) *Cyberpsychology & Behaviour* 237, 242.

[82] Ibid 237.

In Australia, recent news sources report that internet addiction requires more studies before it can be classified as primary mental health issue.[83] This thesis will briefly examine some of these areas to support the rationale for focusing on a specific area intersecting between privacy and workplace law. This focus will fill a gap in the literature with reference to an individual's expectations of privacy and security in relation to information or comments made about work-related matters on their personal SMedia accounts.

1.2.5. Identity theft

The definition of identity theft has no common consensus.[84] The chief security officer of NetLok Inc, a prominent cybersecurity company in the US, opines that commonly held understandings of 'identity theft' are too narrow (eg, theft of online information including email addresses, passwords, credit card details and social security numbers).[85] He notes that a hacker or thief who steals such information often does so to control the victim and is not merely using the information for outright financial gain, such as online shopping.[86] The example he provides of control-based gain is of a thief who hacks into a dentist's records, discovers that the dentist has HIV and uses that information to blackmail the dentist by threatening to inform the dentist's clients.[87]

---

[83] Mary Pascaline Dharshini, 'Vitality: Internet Addiction May Lead to More Mental Health Problems Study Finds', *Medical Daily* (online), 19 September 2016 < http://www.medicaldaily.com/internet-addiction-internet-usage-mental-health-depression-and-anxiety-398216>.
[84] Australian Law Reform Commission, *Australian Privacy Law and Practice*, Report No 108 (2008) [12.3]–[12.4].
[85] Ian Lopez, 'Happy Holidays — Tis the Season for Identity Theft: Consumers and Law Firms Need Increased Vigilance Against More Sophisticated Hackers' (2015) 38(14) *National Law Journal* 18.
[86] Ibid.
[87] Ibid.

The implication that may be taken from this is that identity theft is moving from impersonal financial loss to a more targeted and control-based victimisation against individuals, with the actual identity theft being a means to cause more than mere financial loss. A 2014 survey by the US Bureau of Justice[88] that used the narrower and more common definition of identity theft, recorded that 86 per cent of victims (aged 16 years and older) of identity theft reported only financial loss due to the theft. The statistics show that the number of elderly victims of identity theft in the US increased from 2.1 million in 2012 to 2.6 million in 2014.[89] Research proposes that the elderly may have low impulse control and; therefore, expose themselves to an avoidably higher degree of risk to identity theft when they make internet purchases from unverified vendors.[90] However, the elderly described in this instance are not the focus of this paper, as the research is based on retirees and not current members of the workforce.

In Australia, the Australian Law Reform Commission (ALRC) also states that there is no clear definition of 'identity theft'.[91] It uses the following terminology to discuss the concept: identity crime, identity fraud and identify theft. The ALRC considers 'identity crime' as a broader concept, encompassing any criminal act carried out that uses 'fabricated, manipulated or stolen identity'.[92] In this instance, fabricated means

[88] Erika Harrel, *Victims of Identity Theft, 2014* (27 September 2015) Bureau of Justice Statistics <https://www.bjs.gov/index.cfm?ty=pbdetail&iid=5408>.
[89] Ibid.
[90] Kirsty Holtfretera et al, 'Risky Remote Purchasing and Identity Theft Victimization Among Older Internet Users' (2015) 21(7) *Psychology, Crime and Law* 681.
[91] Australian Law Reform Commission, *Australian Privacy Law and Practice*, Report No 108 (2008) [12.3].
[92] Australasian Centre for Policing Research and Australian Transaction Reports and Analysis Centre Proof of Identity Steering Committee, *Standardisation of Definitions of Identity Crime Terms: A Step Towards Consistency* (2006) 15, cited in Australian Law Reform Commission, *Australian Privacy Law and Practice*, Report No 108 (2008).

the creation of a new or previously non-existent identity. This is relevant when we examine the remaining definitions below.

Identity fraud is defined more narrowly as akin to, though not the same as, the common understanding of identity theft described earlier. Thus, identity fraud includes utilising an imaginary *non-existent* or *stolen* identity.[93] Identity fraud is a type of identity theft; however, it is considered separately in the ALRC Report.[94] The ALRC refers to 'identity theft' as an unlawful assumption or 'takeover' of an individual's *pre-existing* identity.[95] The victimised individual may be living or dead. Alternatively, 'identity theft' can also refer to the assumption of the identity of an existing artificial legal entity such as a corporation.[96] In this instance, the person or persons who have created the assumed identity use it to commit an unlawful act. Examples include using the stolen identity for personal gain such as accessing financial services or online shopping.

One clear example of the commission of identity fraud is the case of the Singaporean national who lived in the US and practiced immigration law from 2006 to 2009.[97] He had faced criminal charges of fraud in Singapore when he applied for a passport using another person's details. He used the passport obtained by identity fraud to

---

[93] Australian Law Reform Commission, *Australian Privacy Law and Practice*, Report No 108 (2008) [12.4].
[94] Ibid.
[95] Ibid, citing Australasian Centre for Policing Research and Australian Transaction Reports and Analysis Centre Proof of Identity Steering Committee, *Standardisation of Definitions of Identity Crime Terms: A Step Towards Consistency* (2006) 15.
[96] Australasian Centre for Policing Research, *Australasian Identity Crime Policing Strategy 2006–2008 of the Australasian and South West Pacific Region Police Commissioners' Conference* (2005) 1, cited in Australian Law Reform Commission, *Australian Privacy Law and Practice*, Report No 108 (2008).
[97] Selina Lum, 'S'porean Fugitive Lived a Lie in US as a 'Lawyer' for Years', *Straits Times* (online), 19 May 2016 <http://www.straitstimes.com/singapore/courts-crime/sporean-fugitive-lived-a-lie-in-us-as-lawyer-for-years>.

flee Singapore for the US where he is alleged to have used as many as seven aliases.[98] An alias is a false or assumed identity that may be stolen from a pre-existing identity or simply created.[99] An example of a non-fraudulent alias is a pseudonym. A negative, fraudulent or illegal example of an alias is the case of the Singaporean using the particulars of another person to obtain a passport.

Through bodies such as the ALRC, Australian policymakers are mindful of the threat of identity theft to individuals and industry. They are trying to differentiate the crime between instances in which the theft is of pre-existing identities compared with situations in which criminals create new and false identities. This may be because the internet provides opportunities for individuals to create such 'new' identities, particularly in the area of SMedia in which people may have multiple accounts with different or fake public profiles, enabling them to interact and potentially abuse the people with whom they communicate while taking advantage of a level of anonymity.[100]

Research regarding identity theft is not new. More than a decade ago, Milne, Rohm and Bahl discussed consumer behaviour related to identity theft through the analysis of three varying consumer groups.[101] Their study examined demographic behaviours and attitudes as a means to determine the criteria that policymakers should consider in enhancing the protection of online data and the prevention of identity theft.

---

[98] Ibid.
[99]Cambridge Dictionary, *Cambridge Academic Content Dictionary* (online ed, 2018) 'Alias' extracted 17 January 2018 <http://dictionary.cambridge.org/us/dictionary/english/alias>.
[100] Jason Pelish, '10 Different Types of Fake Facebook Accounts' on Jason Pelish, *The Click* Whisperer (4 April 2014) <https://www.clickwhisperer.com/2014/04/04/the-10-types-of-fake-facebook-accounts/>.
[101] George R Milne, Andrew J Rohm and Shalini Bahl, 'Consumers' Protection of Online Privacy and Identity' (2004) 38(2) *Journal of Consumer Affairs* 217.

However, all the consumer groups they used in their analysis were from the US and this perspective may not be properly representative of the exponentially multicultural, multinational community that is the internet today.

This thesis takes the view that the ALRC recommendations are valuable, even if they are not perfect. However, identity theft is a form of privacy research that is beyond the scope of this thesis. It has been included to demonstrate that this is an area that is well researched. This thesis will focus on employee use of personal SMedia that leads to unfair dismissal. This is an area that is not well researched in the literature. Thus, this thesis will provide a valuable understanding of the direction that Australian courts are moving towards when determining issues on employee privacy with regards to their personal SMedia use.

1.2.6. Privacy and the contemporary employee

The focus of this thesis is on privacy and the workplace. The material reviewed earlier is incidental to the focus of this thesis and is reviewed for the purposes of identifying the gap in contemporary research in this area.

Conventionally, workplace law deals with the issue of balancing employer control with an employee's right to privacy. In Australia, an employee's privacy as it relates to using the employee's personal SMedia accounts while at work is a developing issue. Traditional workplace relationships and the issues that arise from these are primarily governed by legislation, both at Commonwealth[102] and state[103] levels.

[102] See *Fair Work Act 2009* (Cth) pt 3-2.
[103] See *Industrial Relations Act 1979* (WA) s 23A.

Between them, the jurisdictions provide a legislative framework that covers the full range of employment relationships, both public and private.

In addition to the legislative framework, common law principles are utilised by the bodies that adjudicate employer–employee disputes[104] and are often considered by the Fair Work Commission (FWC) when determining unfair dismissal cases.[105] If an employee is found to have not breached a common law duty as well as found to have committed no specific statutory breach, their dismissal will usually be found to have been unfair.[106] One example of a common law principle adopted by the judiciary can be seen is the FWC ruling that the common law duty of loyalty and fidelity is a facet of employment law.[107] Another common law principle still considered good law is the duty of the employee to act in the best interests of the employer.[108] Andrew Frazer, Associate Professor from the School of Law, University of Wollongong, discusses this duty and goes on to accept the House of Lords' (in particular Lord Steyn's) articulation of the duty being an implied responsibility by the employee 'to serve his employer loyally and not contrary to his employer's interests'.[109] Frazer likens it to the employee's contractual duty of fidelity.[110]

---

[104] *Rose v Telstra Corporation Ltd* [1998] AIRC 1592.
[105] *Byrne v Australian Airline* (1995) 185 CLR 410 at 436. The Court referred to the evolution of the employment relationship from the ancient common law status of master and servant to the more recent employment contract position between two parties. McHugh and Gummow JJ observed that the 'evolution in the common law as to the relationship of employment has been seen as a classic illustration of the shift from status (that of master and servant) to that of contract (between employer and employee)'.
[106] See Louise Thornthwaite, 'Chilling Times: Social Media Policies, Labour Law and Employment Relations' (2016) 54 *Pacific Journal of Human Resources* 332.
[107] *Rose v Telstra Corporation Ltd* [1998] AIRC 1592.
[108] *McDonald v South Australia; McDonald v Minister for Education and Child Development* [2017] SASCFC 146.
[109] Andrew Frazer, *The Employee's Contractual Duty of Fidelity* (2015) University of Wollongong Research Online <http://ro.uow.edu.au/lhapapers/2057/>, citing *Mahmud v Bank of Credit and Commerce International SA* [1998] AC 20, 46.
[110] Andrew Frazer, *The Employee's Contractual Duty of Fidelity* (2015) University of Wollongong Research Online <http://ro.uow.edu.au/lhapapers/2057/>.

However, he states that the duty is broader than a mere fiduciary duty.[111] It includes concepts of 'honesty, faithfulness, good faith, confidentiality and trust as befitting the personal nature of the relationship — but always with regard to the nature and purposes of the engagement and the interests of both parties'.[112] Therefore, the common law duty is limited by the extent and nature of the employment relationship.

Similarly, the contractual duty may be restricted to the scope and ambit of the terms of the contract.[113] Neither the contractual nor the common law duty of employee fidelity creates an unfettered loyalty to the employer.[114] However, fiduciary duties are absolute and require the subsuming of one's interest to further the interests of the party to whom the fiduciary duty is owed.[115] Frazer distinguishes these duties by stating that contractual fidelity protects the employer by serving the mutual intentions of both employer and employee,[116] whereas the common law duty of fidelity operates to find a balance between the individual as an employee and also the employee's interest in improving 'their own human capital for future employability'.[117]

Conversely, in *Commonwealth Bank of Australia v Barker* (2014) 253 CLR 169 the High Court of Australia was reluctant to imply the common law duty of mutual trust

---

[111] Andrew Frazer, *The Employee's Contractual Duty of Fidelity* (2015) University of Wollongong Research Online <http://ro.uow.edu.au/lhapapers/2057/>, citing *Bray v Ford* [1896] AC 44, 51 per Lord Herschell; Robert Flannigan, 'The Boundaries of Fiduciary Accountability' (2004) 83 *Canadian Bar Review* 35; Robert Flannigan, 'Access or Expectation: The Test for Fiduciary Accountability' (2010) 89 *Canadian Bar Review* 1, 4, 11.
[112] Frazer, above n 109.
[113] Ian Curlewis, *Commission Confirms That There is No Contractual Right to Dismiss 'At Will' in Australia* (9 November 2017) Lavan <https://www.lavan.com.au/advice/employment_safety/commission-confirms-that-there-is-no-contractual-right-to-dismiss-at-will-i>.
[114] Frazer, above n 109.
[115] Ibid, citing Mark Freedland, *The Personal Employment Contract* (Oxford University Press, 2003), 176–7.
[116] Frazer, above 109, citing *Vestergaard Frandsen A/S v Bestnet Europe Ltd* [2013] UKSC 31 [44].
[117] Frazer, above n 109.

and confidence.[118] This common law duty is a mutual duty owed by both parties to each other to preserve the integrity of and confidence in the relationship.[119] While the courts may not imply this mutual duty, employers owe common law duties to their employees. An employee's perception that there has been a breach of the employer's duty to provide a safe environment, systems of work and competent fellow employees and reasonable remuneration are often the cause of complaints made by employees on Facebook.[120] These seemingly private complaints can lead to dismissal and, when challenged, these dismissals may be found to be unfair. To determine how the court views such dismissals, these duties together with examples of cases that relate to them will be discussed in Parts 2 and 3 of this thesis.

1.2.7. Contemporary workplace privacy

As will be discussed further in this thesis, privacy is not an entrenched right in Australia. There is some measure of protection for an employee's privacy at the workplace through workplace legislation.[121] However, this is limited to data protection rather than an active protection of an individual employee's right to privacy. This is because the *Act* is not specifically designed to protect employees. It is enacted to protect individual data or personal information that leads to the identification of an individual from being released without their knowledge or consent.[122]

---

[118] *Commonwealth Bank of Australia v Barker* (2014) 253 CLR 169.
[119] Beatrix M P van Dissel, 'Social Media and the Employee's Right to Privacy in Australia' (2014) 4(3) *International Data Privacy Law* 222, 224, citing Rosemary Owens, Joellen Riley and Jill Murray, *Law of Work* (Oxford University Press, 2nd ed, 2011).
[120] See *O'Keefe v Williams Muir's Pty Ltd* [2011] FWA 5311.
[121] *Privacy Act 1988* (Cth).
[122] Section 2A of the *Privacy Act 1988* (Cth).

Twentieth century individual rights are caught in a digital dichotomy. An employer has the ability to find information about an employee through the internet without an employee's knowledge. For example, this can be done as easily as performing an internet search of an employee's name, their email address or looking up an SMedia profile.[123] Pipl is one example of a website that operates to specifically search for people and their SMedia profiles.[124] Thus, access to 'private' information is easy and this raises the question of whether or not the information is actually private. This also raises questions about what an employer or potential employer can do with the information they retrieve.

It is only recently that the repercussions of an individual employee's use of personal SMedia have begun to be recognised as an area in which conventional employment protections alone may not be sufficient.[125] In the absence of clear legislation in the area, the reference to common law principles by the bodies that adjudicate employer–employee disputes are important, as it is the common law that is regarded as having an innate power to create a right to employee privacy in Australia.[126] As can be seen from the High Court's decision in *Commonwealth Bank of Australia v Barker,* is unclear whether the bodies that adjudicate on these matters will choose to use their innate power to imply, entrench or create common law rights.[127]

[123] Jacinta Buchbach, 'Regulating the Boundary Between Work and Self: Emerging Legal Tensions Around Social Media in the Workplace' (Paper presented at the 15th Annual Meeting of the Association of Internet Researchers, Daegu, Korea, 22–24 October 2014).
[124] Pipl, home page <https://pipl.com>.
[125] Thornthwaite, above n 105.
[126] *ABC v Lenah Game Meats Pty Ltd* [2001] 208 CLR 199.
[127] *Commonwealth Bank of Australia v Barker* (2014) 253 CLR 169.

Another reason that may explain the lack of rigorous academic research in the specific area of employment and use of SMedia by employees is that many employment relationships are governed by employment contracts. Therefore, the established areas of contract law and agreed mutual obligations set out the parameters of discussion in the event of an employer–employee dispute.[128] It is only recently that the specific area of the employer's right to scrutinise and discipline an employee's conduct on SMedia platforms has become an issue.[129] From a contractual point of view, scrutiny is required in the area of express or implied terms that may be incorporated into an employment contract through the employer's SMedia policy.[130] The implications of contract, and in particular the effect of an employer's SMedia policy, are discussed further as part of the review of strategies to overcome employees' SMedia related solecisms that result in adverse publicity for employers.

As mentioned earlier, the current lack of academic research on employment and SMedia use by employees is due to the focus on the challenges to individual privacy and human rights infringements through pre-hiring screening of prospective employees, data protection and cybersecurity at the workplace. Another area of research that intersects between the workplace and personal use of SMedia is the use of SMedia for advertising and marketing.[131] Other areas that are parallel to the

[128] Ibid 169.
[129] Daniel Ornstein, 'Social Media Usage in the Workplace Around the World — Developing Law and Practices' (2012) 13 *Business Law International* 195.
[130] Ibid.
[131] See Edward C Malthouse, 'Managing Customer Relationships in the Social Media Era: Introducing the Social CRM House' (2013) 27(4) *Journal of Interactive Marketing* 270; Joonas Rokka, Katariina Karlsson and Janne Tienan, 'Balancing Acts: Managing Employees and Reputation in Social Media' (2014) 30(7–8) *Journal of Marketing Management* 802.

workplace and involve SMedia use include the use of SMedia platforms to participate in national security breaches,[132] cyberterrorism,[133] child pornography[134] and other criminal activities. Among the many areas of focus of industry, academic and legal researchers are data privacy issues both within and across international borders,[135] collection of data about users by SMedia companies and the implications of such collection[136] and the use and abuse of the information collected.[137] Some socio-psychological areas that impinge on the borders of privacy issues include cyberbullying in schools[138] and suicide games such as Blue Whale,[139] while body image issues[140] that involve 'slut shaming' and 'fat shaming'[141] are also areas of interest.

---

[132] Norman Vasu and Benjamin Ang, *CO16312 — Society, Technology and National Security* (23 December 2016) S Rajaratham School of International Studies, Nanyang Technological University <https://www.rsis.edu.sg/rsis-publication/cens/co16312-society-technology-and-national-security/#.Whkx90xL3BI>.

[133] Farzan Kolini and Lech Janczewski, 'Clustering and Topic Modelling: A New Approach for Analysis of National Cyber Security Strategies' (Paper presented at Pacific Asia Conference on Information Systems (PACIS), Langkawi, Malaysia, 16–20 July 2017).

[134] Dorothy L Espelage and Jun Sung Hong, 'Cyberbullying Prevention and Intervention Efforts: Current Knowledge and Future Directions' (2016) 62(6) *Canadian Journal of Psychiatry* 374.

[135] 'Global Overview' (2016) 3 *Privacy, Data Protection and Cybersecurity Law Review* 1–5 (ed) Alan Charles Raul (Law Business Research Ltd, London 2016). This is an example of a comprehensive publication which is published as an annual edition which encompasses issues related to data privacy and protection across the world. This issue includes research from 27 jurisdictions including EU, APEC, Australia, Belgium, Brazil, Canada, China and France.

[136] Kathryn C Montgomery, Jeff Chester and Tijana Milosevic, 'Children's Privacy in the Big Data Era: Research Opportunities' (2017) 140(2) *Pediatrics*.

[137] Jungwoo Ryoo, 'Big Data Security Problems Threaten Consumers' Privacy', *The Conversation*, 23 March 2016 < https://theconversation.com/big-data-security-problems-threaten-consumers-privacy-54798>. Jungwoo Ryoo is an Associate Professor of Information Sciences and Technology at Altoona campus, Penn State University.

[138] Robin M Kowalski and Megan E Morgan, 'Cyberbullying in Schools' in Peter Sturmey (ed), *The Wiley Handbook of Violence and Aggression* (John Wiley & Sons, 2017) vol 3, 1–12.

[139] Paul W C Wong, Gilbert K H Wong and Tim M H Li, 'Suicide Communications on Facebook as a Source of Information in Suicide Research: A Case Study' (2017) 8(1) *Suicidology Online* 1; Richa Mukhra et al, 'Blue Whale Challenge: A Game or Crime?' (2017) *Science and Engineering Ethics* 1.

[140] Rachel Andrew, Marika Tiggemann and Levina Clark, 'Predicting Body Appreciation in Young Women: An Integrated Model of Positive Body Image' (2016) 18 *Body Image* 34.

[141] Mina Park, Yao Sun and Margaret L McLaughlin, 'Social Media Propagation of Content Promoting Risky Health Behaviour' (2017) 20(5) *Cyberpsychology, Behaviour, and Social Networking* 278.

1.3. Current Focus of Research Relating to Employment Law and SMedia

The next question to be addressed in this thesis is the main focus of current academic research around the issues of employment law and SMedia. This part of the literature review discusses and reviews current academic literature in areas in which employee use of SMedia intersects with the workplace environment and relevant employment law principles. This section demonstrates the gap in existing academic research that the thesis will later address. It begins with a discussion of pre-employment scenarios and the growing area of pre-hiring screening practices whereby employers access an employee's personal SMedia with the aim of using the information obtained as a tool for hiring or recruitment evaluation.

1.3.1. Pre-hiring practices

The law as it exists in Australia does not expressly prohibit prospective employers from accessing any information that is publicly available from a potential employee's SMedia accounts. However, the implications of using information that is obtained through online SMedia activities to decide whether to hire or reject a potential employee are still unsettled in the law.[142] It is a grey area because there is no clear legislation or definitive case law on this topic. In an article,[143] Murray Brown examines the *Act*, the *Information Privacy Principles* (*IPPs*) that apply to public sector employers and the *National Privacy Principles* (*NPPs*) that apply to private

[142] Murray Brown, 'Applying for a Job with Big Brother: Is Online Vetting of Job Applicants Lawful in Australia?' (2012) 37(3) *Alternative Law Journal* 186.
[143] Ibid.

entities. Since March 2014, the *Act*, the *IPPs* and the *NPPs* are collectively known as the *APPs*.[144] Brown discusses the limitations that are placed on employers when collecting such information and the extent to which they can use the information to reject potential employees.[145] Conceding that the legislation imposes some requirement for an employer to obtain a prospective employee's consent prior to accessing the prospective employee's personal information, Brown concludes that Australia provides no clear protection against employers accessing employees' SMedia as part of the hiring pre-hiring screening process.[146]

There is one school of thought that theorises that an employer's action of accessing a potential employee's SMedia and viewing any information contained therein may result in the employer being exposed to an action under the *Fair Work Act 2009* (Cth).[147] An employer who has viewed the information on the potential employee's SMedia accounts and decides to hold, not proceed with or reject the said potential employee's application may expose themselves to a claim under the adverse action and general protections provisions in s 342 of the *Fair Work Act 2009* (Cth).[148] Such liability arises because the *Fair Work Act 2009* (Cth) specifically identifies discrimination that results in a refusal to hire a prospective employee as an adverse action.[149] This appears to place the employer in a vulnerable position when attempting to pre-screen employees through their SMedia activities by reversing the

[144] *Privacy Act 1988* (Cth).
[145] Brown, above n 141.
[146] Ibid; and s 27 of the *Privacy Act 1988* (Cth).
[147] Rima Newman, Kristopher Cook and Zoe Brick, 'The Risks of Using Social Media to Screen Job Candidates', *Lexology*, 17 May 2016 *<https://www.lexology.com/library/detail.aspx?g=5e6172ce-f5f5-471a-ab1f-2a6f12ff0ca4>.*
[148] Section 342 of the *Fair Work Act 2009* (Cth).
[149] Section 351(1) of the *Fair Work Act 2009* (Cth).

burden of proof.[150] Legislation places the burden of proof on the employer to show that the decision not to proceed with the individual's employment application was not discriminatory.[151] When hearing such actions, the court will take into account the information available on the potential employee's SMedia that was open for viewing by the employer.[152]

Some potentially discriminatory factors include age, gender, sexuality, political or religious belief, marital or familial status and disability.[153] However, before the burden of proof is passed to the employer, the court will require a potential employee to demonstrate an objective belief that they were rejected due to some discrimination arising as a result of the prospective employer accessing information through their SMedia.[154] In 2014, the Queensland Civil and Administrative Tribunal held an employer liable under the *Queensland Anti-Discrimination Act 1991* (Qld) for requesting information about the applicant's birth date and gender in an online application form.[155] The employer was ordered to pay $5000 in compensation to the individual.[156]

If Brown's conclusion is accepted that Australia provides no clear protection against employers accessing employees' SMedia as part of the pre-hiring screening process

[150] Section 361 of the *Fair Work Act 2009* (Cth).
[151] Ibid.
[152] Rima Newman, Kristopher Cook and Zoe Brick, 'The Risks of Using Social Media to Screen Job Candidates', *Lexology*, 17 May 2016 *<https://www.lexology.com/library/detail.aspx?g=5e6172ce-f5f5-471a-ab1f-2a6f12ff0ca4>.*
[153] *Willmott v Woolworths Ltd* [2014] QCAT 601, in which Woolworths was held to have contravened the *Anti-Discrimination Act 1991* (Qld) ss 7, 8 and 124 by requiring information about the applicant's date of birth and gender in the online job application. The defence under s 209 was held not to apply on the facts.
[154] *Jones v Queensland Tertiary Admissions Centre Ltd* (No 2) (2010) FCA 339 [10].
[155] *Willmott v Woolworths Ltd* [2014] QCAT 601.
[156] Ibid.

it may indicate that, unless the courts or legislation step in, the burden of protecting individual privacy belongs to the employee. One argument that supports this rationale is that most SMedia platforms including Facebook and emerging SMedia sites Instagram,[157] Snapchat[158] and WhatsApp[159] have privacy settings that allow the user (the potential employee) to control who can access their SMedia profile and the material they post. This is done through the user's choice of SMedia platforms that they use and their choice to utilise all available privacy protection settings. This will be discussed in detail following the analysis of case law later in this thesis.

It appears that SMedia platforms are becoming more aware of the privacy issues that surround their users' posts. WhatsApp is a recent example of an SMedia application that has enhanced its security and privacy settings. WhatsApp has implemented automatic encryption of messages sent by a user.[160] Essentially, this is a software security feature that prevents messages within a WhatsApp chat or conversation from being accessed or accessible by anyone who is not in the particular conversation.[161] This feature is automatically activated and cannot be turned off by the user. Each individual message has its own specific security encryption feature[162] that aims to protect the privacy of a user's communications by encoding a message and rendering it unintelligible to any party who attempts to access the message without authorisation.[163]

---

[157] Instagram, home page <https://www.instagram.com>.
[158] Snap Inc, home page <https://www.snapchat.com>.
[159] WhatsApp Inc home page <https://www.whatsapp.com>.
[160] End-to-End Encryption WhatsApp Inc, home page (2017) WhatsApp Web <https://faq.whatsapp.com/en/general/28030015>.
[161] Ibid.
[162] Ibid.
[163] Nate Lord, 'What is Data Encryption?' on *Data Insider* (27 July 2017) <https://digitalguardian.com/blog/what-data-encryption>.

While WhatsApp's encryption feature is not directly relevant to the usual pre-screening conducted by employers, it is an indication of how seriously SMedia platforms view the protection and privacy of interaction and communication between their users. Such mindfulness results in an increased commitment to protect the privacy of individual users and their information contained within the WhatsApp system and the communications they make through it. The rationale explaining or theorising the reason SMedia sites are committed to protecting individual communications is not within the purview of the present discussion, as it is not directly related to the legality of pre-screening of potential employees. However, the increased protection offered by some SMedia sites leads to a conclusion that the individual employee's concerns, responsibilities and potential resulting liabilities to otherwise secure the privacy of their SMedia posts from online pre-employment screening are being reduced. It also supports this thesis' earlier statement that this trend may be a reason why Australian law is slow to expressly safeguard an individual employee's information in the area of SMedia.

Internationally, the perspective is widely different. There appears to be a more structured legislative approach overseas. For example, in Europe, legal and quasi-legal frameworks have been created to limit or regulate the practice of employers accessing information from prospective employees. Germany has enacted limited data access protection legislation.[164] Its approach is innovative in that it expressly prohibits pre-screening of an employee but allows some forms of post-recruitment

[164] Falk Hagedorn, *Privacy in the Workplace: National Report on Germany* (June 2011) <http://pawproject.eu/en/sites/default/files/page/web_national_report_germany_en.pdf>; and *Bundesdatenschutzgesetz* [Federal Data Protection Act] (Germany) 14 August 2009, BDSG, 2009, 2814 [32].

screening. For example, an employer is allowed to screen for criminal offences as part of the confirmation of employment.[165]

The UK has best practice standards in place for pre-hiring screening.[166] One example is that an employer is required to obtain the consent of the prospective employee to access information from the prospective employee's SMedia accounts.[167] This suggests that the UK appears to be developing a quasi-legal rather than a strict legal framework to regulate employer pre-screening. The effect of, or advantages and disadvantages of a quasi-legal approach, as compared to pure legal regulation (as in Germany) of pre-hiring screening is beyond the scope of this thesis. A relevant commonality in the jurisdictions of Germany and the UK is that employee consent must obtained prior to such screening being conducted.

In Australia, some industries have best practice standards and formal pre-hiring screenings in place.[168] Some critical industries include mining and public transport (eg, train and ferry services).[169] Screening for drugs in specific industries is justified based on the industry requirements and to ensure workplace safety, productivity and the protection of the public.[170] It appears that the courts are adopting a strict

---

[165] Ibid.
[166] British Standards Institution, *BS 7858:2012 Security Screening of Individuals Employed in a Security Environment. Code of Practice* (31 October 2012) <https://shop.bsigroup.com/ProductDetail?pid=000000000030237324>; Centre for the Protection of National Infrastructure, *Pre-Employment Screening: A Good Practice Guide* (5th ed, 2015) <https://www.cpni.gov.uk/system/files/documents/61/e9/pre-employment-screening-A-good-practice-guide-edition-5.pdf>.
[167] Ibid.
[168] The Privacy Committee of New South Wales, *Drug Testing in the Workplace*, Report No 64 (1992) 7.
[169] For an example of ferry services see *Toms v Harbour City Ferries Pty Ltd* [2014] FWC 2327. For a discussion on pre-hiring screening in the mining industry, see Peter Holland, 'Drug Testing in the Australian Workplace: Still a Contested Terrain' (2016) 58(5) *Journal of Industrial Relations* 688.
[170] Ken Pidd and Ann M Roche, 'How Effective is Drug Testing as a Workplace Safety Strategy? A Systematic Review of the Evidence' (2014) 71 *Accident Analysis and Prevention* 154.

approach towards supporting corporate policies that seek to enforce a 'zero tolerance' rule with regards to the use of intoxicants at the workplace. *Toms v Harbour City Ferries Pty Ltd* [2014] FWC 2327 (*Toms*) provides an example of the FWC supporting an employer's zero tolerance approach.[171] In *Toms* the employee was dismissed due to his drug use.[172] The employee, Toms, had used marijuana for pain relief.[173] He had a good employment record and had only smoked a marijuana cigarette as he was not scheduled to work on the particular day.[174] He was suddenly called to replace another Ferry Master who had taken ill.[175] The ferry Toms was driving hit the quay.[176] The damage incurred by the ferry colliding with the quay was attributed to a process defect (not Toms' intoxication) and resulted in the formulation of new training protocols for all the Ferry Masters.[177] At first instance, the FWC reinstated Toms, as they found that the dismissal was unfair.[178] Later, upon appeal, the Full Bench upheld Toms' dismissal.[179] This case was followed by the Full Bench of the FWC in *Construction, Forestry, Mining and Energy Union — Construction and General Division v Port Kembla Coal Terminal (PKCT)* [2015] FWCFB 4075.[180]

Pidd and Roche theorise that decisions such as *Toms* emphasise the importance courts place on supporting a 'zero tolerance' policy that moves beyond the actual incident in the workplace.[181] Such decisions may indicate that employers can and

[171] *Toms v Harbour City Ferries Pty Ltd* [2014] FWC 2327.
[172] Ibid [13].
[173] Ibid [14].
[174] Ibid [12].
[175] Ibid [14].
[176] Ibid [10].
[177] Ibid [31].
[178] Ibid [83].
[179] *Harbour City Ferries Pty Ltd v Toms* [2014] FWCFB 6249.
[180] *Construction, Forestry, Mining and Energy Union — Construction and General Division v Port Kembla Coal Terminal (PKCT)* [2015] FWCFB 4075 [17].
[181] Pidd and Roche, above n 169.

will discipline employees for actions that occur outside the workplace.[182] Pidd suggests that this control is limited to situations in which safety in the workplace is a crucial element of the employee's job.[183] As a critique, this thesis submits that these types of decisions do affect an employee's life and conduct outside the workplace. On the facts, Toms was on leave with no expectation of being called into work. In addition, he was using the marijuana specifically for medicinal purposes or pain management, not for recreational purposes and not to support any kind of addiction. This thesis takes the view is that there is always the possibility for this apparently limited encroachment into employee privacy, and particularly privacy outside the workplace, to be extended into an employee's use of SMedia. As discussed earlier, the lines between work and personal time are increasingly blurred. The case law discussed below may provide some indication of whether such intrusions into the privacy of the employee will continue.

In certain pre-hiring screenings, testing for drugs requires clear consent from the employee.[184] That said, a job applicant who refuses such a test is not likely to be employed. Allegorically, if a prospective employer asks a prospective employee for consent to access their SMedia account, there is an underlying concern as to whether or not the person, whether currently employed or being considered for employment, has a real and unequivocal right to refuse such a screening as they may fear either losing or not getting the job if they do.[185] An SMedia account is

[182] Saul Harben and Steve Bowler, *Drug and Alcohol Use: When Zero Tolerance is Tolerable* (2 April 2015) Clayton Utz, <https://www.claytonutz.com/knowledge/2015/april/drug-and-alcohol-use-when-zero-tolerance-is-tolerable>.
[183] Pidd and Roche, above n 169.
[184] Section 27 of the *Privacy Act 1988* (Cth).
[185] *Construction, Forestry, Mining and Energy Union — Construction and General Division v Port Kembla Coal Terminal (PKCT)* [2015] FWCFB 4075.

arguably a reflection of an employee's personal or social life as opposed to their professional persona.[186] For that reason, the information in an SMedia account is arguably not relevant to the potential employment. Nonetheless, an applicant's failure to give permission for access may result in them not being considered for the job. At the end of the hiring process, this access to, or use of information obtained, from a prospective employee's SMedia account may raise questions of indirect discrimination. The ALRC is clear that, overall, Australian legislation has broadly identified four primary categories of unlawful discrimination: race, sex, equal opportunity and disabilities.[187] Unlawful discrimination includes 'harm or less favourable treatment resulting from indirect discrimination'.[188]

To be unlawful, discrimination must be based on a specific attribute set out in a particular piece of legislation. For example, discrimination based on gender is unlawful by way of the *Sex Discrimination Act 1984* (Cth). Yet any discrimination that arises from an attribute that is not listed in legislation precludes the victim from applying for a relief under anti-discrimination law.[189] An example given by the ALRC of such a situation is when there is discrimination of a person based on a simple personal dislike by the discriminator.[190] In this context, pre-screening of a prospective employee's SMedia may give rise to something as intangible as a dislike of the type of humour displayed by the prospective employee. If this dislike influences the hiring process, there will be no legal recourse for the said employee

[186] Patricia Sanchez Abril, Avner Levine, and Alissa Del Reigo, 'Blurred Boundaries: Social Media Privacy and the Twenty First Century Employee' (2012) 49(1) *American Business Law Journal* 64.
[187] Australian Law Reform Commission, *Essentially Yours: The Protection of Human Genetic Information in Australia*, Report No 96 (2003) [9.4]–[9.6].
[188] Ibid [9.17].
[189] Ibid [9.18].
[190] Ibid.

as it would be too difficult to prove that the existence of dislike or discrimination was the reason that the applicant was not employed. This raises the question of whether this is a remote likelihood. In the prevailing tumultuous socio-economic climate of Australia, I am of the view that it is unlikely to be too remote.

In the same vein, such pre-hiring screenings may raise allegations of a failure of natural justice or question the fairness of allowing an employer to access or use information that is obtained from an employee's SMedia to determine employment, rather than proceeding based on the employee's qualifications and skill suitability for the position. In the US, there appears to be latitude that allows employers to conduct pre-hiring screening through accessing employees' SMedia accounts if these accounts are available for the potential employer to access. For example, in 2010 a Microsoft-commissioned survey of recruitment professionals in the US showed that nearly 80 per cent of recruiters did online research into the reputation of prospective employees.[191] This may be because there is no definitive national legislative framework in place, nor any clear American jurisprudence.[192] The law that is closest to providing some regulation in this area is in legislation that is related to anti-discrimination. One specific example is the prohibition on employers making hiring or firing decisions based on race, colour, religion, sex or national origin.[193] However, these laws generally relate more to the use of information obtained from pre-hiring

[191] Cross-tab, 'Online Reputation in a Connected World' (January 2010) <download.microsoft.com/.../dpd_online%20reputation%20research_overview.doc>, *Alternative site*: Braak, Nick, 'Online Reputation in a Connected World' *LinkedIn Slideshare* 27 January 2010 <https://www.slideshare.net/nickbraak/online-reputation-in-a-connected-world> cited in Robert Sprague, 'Invasion of the Social Networks: Blurring the Line between Personal Life and the Employment Relationship' (2011) 50(1) *University of Louisville Law Review* 4.
[192] Francois Quintin Cilliers, 'The Role and Effect of Social Media in the Workplace' (2013) 40(3) *Northern Kentucky Law Review* 568.
[193] 42 USC, beginning 2000 Title *VII Civil Rights Act 1964* (Cth).

screening as opposed to the act of accessing a prospective employee's SMedia or other online presence.

According to Buchbach, almost 50 per cent of recruitment personnel in the US examined the SMedia of prospective employees.[194] The paper by Buchbach raises more questions than answers. For example, Buchbach alludes that from an employer's perspective an individual's SMedia profile may provide a greater insight into the individual's fit into the employer's organisational culture.[195] This is not strictly related to an employee's professional competencies and may well open the door of intangible discrimination. However, Buchbach does conclude that resolving employer–employee issues in the digital age requires a more unorthodox methodology, compared with existing legal mechanisms for dealing with the employment relationship.[196]

The above discussion only deals with the pre-recruitment process and does not address the issue of employer control over employee use of SMedia within the employment period that is a later focus in this thesis.

[194] Donald H Kluemper, 'Social Network Screening: Pitfalls, Possibilities, and Parallels in Employment Selection', in Tanya Bondarouk and Miguel R Olivas-Luján (eds), *Social Media in Human Resources Management (Advanced Series in Management, Volume 12)* (Emerald Group Publishing Ltd, 2013), 1; Jacinta Buchbach, 'Regulating the Boundary Between Work and Self: Emerging Legal Tensions Around Social Media in the Workplace' (Paper presented at the 15th Annual Meeting of the Association of Internet Researchers, Daegu, Korea, 22–24 October 2014).
[195] Jacinta Buchbach, 'Regulating the Boundary Between Work and Self: Emerging Legal Tensions Around Social Media in the Workplace' (Paper presented at the 15th Annual Meeting of the Association of Internet Researchers, Daegu, Korea, 22–24 October 2014).
[196] Ibid.

1.3.2. Monitoring or surveillance of employees through their SMedia

Another question is whether employers have a right to monitor an employee's SMedia use if employees are using devices or internet facilities or networks that are provided by the employer. In Australia, the existing privacy legislation is geared to protect personal information of an employee (eg, medical records).[197] The law also includes special provisions covering 'sensitive' information as to a person's race, political, religious and philosophical beliefs, sexual preference and criminal records.[198] The law does not yet deal with situations in which there is private employee use of employer-provided technology.

If the employee uses equipment or facilities that are provided by an employer, the employer's expectation is that employees are to use these only in the best interests and productivity of the employer.[199] The employer's expectation derives from common law duties such as an employee's duty of loyalty.[200] Another duty is the employee's duty to obey lawful and reasonable instructions.[201] Such instructions could be made through corporate policies, SMedia policies and so forth. As discussed earlier, this is in line with the general flow of case law that supports the position that the common law duty of loyalty to an employer should be upheld.[202]

---

[197] *Privacy Act 1988* (Cth); *Australian Privacy Principles*.
[198] Section 51 of the *Privacy Act 1988* (Cth).
[199] Julie de Rooy, 'Workplace Privacy in a Technological Environment' (Paper presented at 6th Computer World Conference, Edinburgh, Scotland, 4–8 September 2006 <http://www.law.ed.ac.uk/ahrc/complaw/papers.asp>.
[200] *Concut Pty Ltd v Worrell* (2000) 176 ALR 693, in which an employee used the employer's materials and fellow employees' skill to construct his personal dwelling was held to be a breach of this duty of faithful service to his employer and valid grounds for dismissal.
[201] *Parmalat Food Products Pty Ltd v Wililo* [2011] FWAFB 1166 [9], [35],[121], in which an employee refused to comply with a company policy or procedure.
[202] Julie de Rooy, 'Workplace Privacy in a Technological Environment' (Paper presented at 6th Computer World Conference, Edinburgh, Scotland, 4–8 September 2006 <http://www.law.ed.ac.uk/ahrc/complaw/papers.asp>.

There is no legislation that expressly prohibits an employer from monitoring an employee's use of SMedia during work.[203] This may be because such monitoring can be seen as an employer ensuring that the employee is upholding the duty of loyalty. Employer monitoring may be an attempt to stop 'cyberslacking', a growing concern in the workforce.[204] Cyberslacking, also known as 'cyberloafing' or 'time banditry', refers to workers who spend (or steal) more time online on non–work-related activities than on work-related activities.[205] In Australia, *O'Connor v Outdoor Creations Pty Ltd* [2011] FWA 3081 is authority that 'excessive use of social media during work hours may constitute a valid reason for the termination of employment'.[206] The cyberslacking phenomenon is not a focus of this thesis as it is not related to the privacy of an employee's information and thus, will not be discussed further.

Despite the lack of protective legislation, an employee may find some rights under the common law. The duty of mutual trust and confidence has been unanimously rejected by the Australian High Court.[207] However, if the employment contract does not have an express clause that authorises the employer or informs the employee of the employer's intention to monitor employees on devices provided by the employer, then the employer may be held to be in breach of the employer's contractual

[203] Dan Jerker B Svantesson, 'Online Workplace Surveillance — The View from Down Under' (2012) 2(3) *International Data Privacy Law* 179.
[204] Wilnelia Hernández, Yair Levy and Michelle M Ramim, 'An Empirical Assessment of Employee Cyberslacking in the Public Sector: The Social Engineering Threat' (2016) *CEC Faculty Articles* 340 <http://nsuworks.nova.edu/gscis_facarticles/340>.
[205] Emily Lowe-Calverley and Rachel Grieve, 'Web of Deceit: Relationships Between the Dark Triad, Perceived Ability to Deceive and Cyberloafing' (2017) 11(2) *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 5.
[206] *O'Connor v Outdoor Creations Pty Ltd* [2011] FWA 3081.
[207] *Commonwealth Bank of Australia v Barker* (2014) 253 CLR 169.

obligations.[208] It can be argued that an employee using employer-provided devices has a reasonable expectation of privacy unless otherwise informed.[209] In the US, a 'reasonable expectation of privacy' has been formulated as a two-step process: 'First, the claimant must have a subjective expectation of privacy. Second, there must be a legitimate expectation of privacy which society accepts and legitimises'.[210] The former is deemed to be based on the contractual obligations of the parties.[211] The latter is broader and dependent on the social and cultural norms of the region or country.[212] For example, in a country like the US where individual freedoms are considered important a high level of employer intrusion may lead to higher levels of worker stress and a decline in productivity.[213] Whether Australian law allows employees to raise 'a reasonable expectation of privacy' is unclear. This will be discussed in Part 3, in relation to unfair dismissals that resulted from employers monitoring employees' SMedia.

1.3.2.1. Effect of deleting records of use on an employer-provided device

The next situation to be examined is when an employee uses a device provided by an employer for a personal purpose but later deletes records of that use. Sometimes employees use devices provided by an employer for personal use and then delete the email or clear the internet browser history to remove traces of such use.

[208] Ronald McCallum and Andrew Stewart, 'The Impact of Electronic Technology on Workplace Disputes in Australia' (2002) 24(19) *Computer Labor Law and Policy Journal* 36.
[209] Sanchez Abril et al, above n 185, 71.
[210] Ibid.
[211] Jeffery M Stanton, 'Traditional and Electronic Monitoring from an Organizational Justice Perspective' (2000) 15 *Journal of Business & Psychology* 129, 130, 142–5, cited by Patricia Sanchez Abril, Avner Levine and Alissa Del Reigo, 'Blurred Boundaries: Social Media Privacy and the Twenty First Century Employee' (2012) 49(1) *American Business Law Journal* 71.
[212] Ibid.
[213] Ibid.

However, copies and remnants of deleted emails and prior online activity of an employee can remain on the device and employers may access these to track employee activity using specific technology known as desktop logging systems.[214]

One example from case law is when a public employee accessed pornography using an employer-provided device (ie, a laptop).[215] This activity occurred over a period of three weeks and the employee deleted all traces of the access from the device's internet browser history.[216] However, his conduct was discovered when his employer conducted a standard operational check on the device and software installed on the device.[217] The employee clearly intended his actions to be private. On the facts, the employee was found to be in breach of a clear work policy for which the employee had signed his acceptance.[218] The policy prohibited employees from using the employer-given facilities to access pornography.[219] This raises the spectre of potential breaches of privacy. For example, when employers monitor employee behaviour and discover personal information relating to the employee under the umbrella of safeguarding or enforcing corporate policy, in this instance a policy against pornography.

The question for the employee may be whether the employer had granted the employee a reasonable expectation to privacy.[220] In *City of Ontario v Quon* 130 (2010) S Ct 2619, a police officer claimed invasion of privacy when his employer

[214] See *Griffiths v Rose* (2011) 192 FCR 130, 133, discussing Spector360 software, a type of desktop logging system.
[215] Ibid 132.
[216] Ibid 133.
[217] Ibid 133.
[218] Ibid 138.
[219] Ibid 138.
[220] Above n 208.

scrutinised the personal messages he sent on the pager provided by his employer.[221] The Supreme Court of the United States was cautious in its approach. It took the view that a balance may need to be found between the need for privacy and rapid advances in technology.[222] The Court stated that these rapid changes in technology are re-shaping boundaries of privacy expectations between employees and employers.[223] Sanchez et al are of the view that this question is usually answered by examining the surrounding circumstances of the particular employer–employee relationship.[224] This thesis agrees with Sanchez et al, and argues that the surrounding circumstances are factors that should also be considered in the Australian context. As stated earlier, a factor to be considered is whether there is an express authorisation by the employee that allows the employer to access all records of any communication carried out using the employer-provided device.

A recent decision of the European Court of Human Rights appears to narrowly interpret the boundaries of employer monitoring of employee communication. In September 2017, the Grand Chamber of the European Court of Human Rights upheld an employee's appeal to privacy under Article 8 of the European Convention of Human Rights.[225] Article 8 provides that an individual has a right to privacy for their private and family life, home and correspondence.[226] The Grand Chamber determined that an employee's termination due to his employer monitoring his use

[221] *City of Ontario v Quon* 130 (2010) S Ct 2619, 2625; Patricia Sanchez Abril, Avner Levine and Alissa Del Reigo, 'Blurred Boundaries: Social Media Privacy and the Twenty First Century Employee' (2012) 49(1) *American Business Law Journal* 71.
[222] Ibid.
[223] Ibid.
[224] Sanchez Abril et al, above n 185, 68.
[225] *Barbulescu v Romania* [2017] ECHR 754.
[226] Article 8 of the *European Convention on Human Rights*.

of his Yahoo professional and personal messenger accounts without his express consent was improper.[227] The employee had used his personal Yahoo Messenger account to message his brother and his fiancée while he also messaged work-related matters on the separate Yahoo Messenger account set up for that purpose by his employer.[228] Both actions were conducted during work time.[229] The employer had, in line with the company's SMedia policy, monitored the employee and extracted some communication that included the personal communication.[230] Among other items, the employer's SMedia policy prohibited the use of employer resources for personal use.[231] The employee claimed that his privacy had been breached.[232]

The Grand Chamber of the European Court of Human Rights upheld this claim on the following grounds. The Grand Chamber found that, on the facts, the employer had placed its interests to safeguard company rights over the employee's right to privacy of communication under Article 8.[233] Among the facts that the Grand Chamber considered was the employer's failure to justify the precise reason as to why the employee's communications were being monitored.[234] Another consideration was whether the employer could have used less intrusive ways of monitoring that would have limited the access of their monitoring from encroaching into the employee's personal communications.[235] The Grand Chamber also stated

[227] *Barbulescu v Romania* [2017] ECHR 754.
[228] Ibid [21].
[229] Ibid [7].
[230] Ibid [7].
[231] Ibid [10].
[232] Ibid [7].
[233] Ibid [7].
[234] Ibid [7].
[235] Ibid [7].

that to validly monitor an employee's communications, the employer should inform the employee of the full scope and ambit of their proposed monitoring policy prior to commencing such monitoring.[236] The facts in this decision are similar to the Canadian case of *City of Ontario v Quon* 130 (2010) S Ct 2619, 2625, in which the court found that despite the employer having in place a clear SMedia policy of which the aggrieved employee was fully aware, the employer's access of the employee's personal messages on the employee's personal SMedia account without the employee's express consent or knowledge was held to be a breach of that employee's privacy.[237]

The above two cases from jurisdictions as diverse as Europe and the US appear to indicate a narrow interpretation of how and when an employer may monitor the communications of an employee — even when those communications are on devices given by employer[238] or on SMedia sites set up for work purposes.[239] In Australia, the situation is more complicated as there is no overarching protection of employee communication.[240] Following the 2014 amendments that replaced the *NPPs* and *IPPs* with the now generic *APPs*, only employee records and personal information related to an employee are exempt from the *Act*. Forsyth, a researcher and a lawyer, takes the view that this is a murky area and two questions need to be answered before anyone can determine if the disputed communication falls within the exemption of the *Act*.[241] First, does the communication contain personal

[236] Ibid [7].
[237] Above n 220.
[238] *Barbulescu v Romania* [2017] ECHR 754.
[239] Above n 220.
[240] Thornthwaite, above n 16, 164.
[241] Anthony Forsyth, 'A Thin Wall of Privacy Protection, with Gaps and Cracks: Regulation of Employees' Personal Information and Workplace Privacy in Australia' in Roger Blanpain (ed),

information (eg, some detail that enables the employee to be identified such as their name)? If it does, the *Act* may protect the employee's communication.[242] Second, does the employee's communication fall within the definition of an 'employee record' in the *Act*? If it does, then potentially the exemption to the *Act* applies and the communication may be open to employer scrutiny. Forsyth notes that SMedia policies and their effect on employee privacy are yet another factor that complicates this issue. Forsyth summarises the complexities of determining whether an employee can be monitored or if the information that is obtained through such monitoring can be used against the employee and notes that it is a legal minefield for employers.[243]

Another factor that may be relevant is the nature of the industry in which the work relationship exists. For example, the banking and securities industries have strict industry guidelines about employee use of employer-provided devices.[244] The Commonwealth Bank of Australia (CBA) has a SMedia policy that appears to render an innocuous comment made by an employee about teacups in the workplace as a potential breach of the policy.[245] Item 4 of the *CBA Social Media Policy* requires employees to report any comments by their respective SMedia connections that may be not complimentary to CBA.[246] More concerning is that Item 4 of the Policy seemingly renders employees responsible for the comments or opinions of others

'Protection of Employees' Personal Information and Privacy' (2014) 88 *Bulletin of Comparative Labour Relations* 7.

[242] Sections 13 and 14 of the *Privacy Act 1988* (Cth).

[243] Ibid 24.

[244] Commonwealth Bank of Australia, *CBA Social Media Policy* (1 December 2010) <https://www.google.com.au/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiW7ZiZ8cnXAhUCy7wKHRuXCTkQFggoMAA&url=http%3A%2F%2Fcommetrics.com%2Fdownload%2F37%2F&usg=AOvVaw1QPkYpp3H4Oa-JV0u0wTJB>.

[245] Ibid.

[246] Ibid.

on their SMedia connections. If a SMedia connection's comment is negative or against CBA, the employee may be considered in breach of the policy.[247] The Financial Services Union has taken umbrage about this policy and is in ongoing negotiations with CBA to have the policy altered.[248] From an employee perspective, this level of employer control is excruciatingly challenging to comply with. It appears to require that employees of CBA sacrifice SMedia activity to avoid risk of breaching of the policy. The right to freedom of association, discrimination and other potential human rights issues are all relevant to the operation of such a policy and are provided for in various Australian legislation and case law as discussed in Part 2 of this thesis. To date, there has been no case law concerning the application of the *CBA Social Media Policy*. We can only speculate whether CBA applies the policy in a strict matter or if it approaches SMedia issues more realistically than its policy suggests.

Other industries that utilise SMedia either directly or indirectly may allow much more latitude for employees to use SMedia for personal purposes. One example is Google.[249] Google's approach is at the opposite end of the spectrum compared with the conservative approach taken by CBA. Google appears to penalise employees who do not aggressively utilise their SMedia accounts to encourage their contacts to use Google as their preferred mode of online interaction.[250] The penalty is through

[247] Jeffry Pilcher, 'Banks Social Media Policy Says Snitch & Spy on Your Friends or You're Fired' (7 February 2011) *The Financial Brand* <https://thefinancialbrand.com/16718/commonwealth-bank-social-media-policy/>.
[248] Ibid.
[249] Nicholas Carlson, 'Larry Page Just Tied ALL Employees' Bonuses to the Success of Google's Social Strategy', *Business Insider* (online), 7 April 2011 <http://www.businessinsider.com/larry-page-just-tied-employee-bonuses-to-the-success-of-the-googles-social-strategy-2011-4>.
[250] Ibid.

performance appraisals and the volume of employee contacts that interact through Google might well be a key performance indicator for bonus allocations.[251]

SMedia policies, and how these are viewed by employers, employees and bodies that adjudicate employer–employee disputes in determining unfair dismissals due to SMedia use, will be discussed in depth later in this thesis as part of the analysis of case law.

[251] Ibid.

Part 2: Privacy and Australian Employees

This discussion is distinct from Part 1 of this thesis that identifies the knowledge gap this thesis will fill. Part 2 deals with contemporary perceptions of privacy, especially in relation to the areas of digital and SMedia platforms. The recurring theme in this discussion about SMedia and digital research centres on the employee's right to privacy when utilising their personal SMedia accounts.

It is important to determine the scope, if any, of the duties that employees owe to their employer when using their personal SMedia at work or away from work. Whether an employee has rights to privacy that may prohibit an employer from accessing or taking action against an employee for comments they make on SMedia must be considered. Answering these questions will help determine the level of restraint required from an employee in relation to the employee's 'freedom' of speech when communicating opinions about their work, employer or any other related matters through their personal SMedia. These questions will form the foundation for the analysis of judicial decisions and descriptions of current trends in dealing with the issues surrounding personal SMedia and the employment relationship. This analysis is presented in Part 3.

In answering the above questions, Part 2 will discuss the following:

- contextual definitions of privacy — a brief examination defining the idea or notion of privacy as it has evolved over time and the current prevailing views with regard to online privacy that are relevant to this thesis

- the Australian position on privacy — an overview of the legislation and case law that relates to privacy in Australia.

2.1. Contextual Definitions of Privacy

For the context of this thesis, notions of privacy can be separated into two distinct zones. These zones are spatial privacy and personal privacy.

2.1.1. Spatial privacy

Spatial privacy is contextualised as a right to or about property that includes a definitive space used, managed or controlled exclusively by an individual. In the context of this thesis, spatial privacy will include the virtual online space of SMedia sites used by employees.

More commonly, spatial privacy is exemplified as a physical space. This is evidenced by common adages such as ‘a man’s home is his castle’ or ‘good fences make good neighbours’ and is well accepted in doctrinal notions of privacy. As far back as the Talmud, an official of the court was not allowed to enter the home of a judgment debtor to seize money for a creditor.[252] Similarly, the Quran prohibits entry into a person’s home without the agreement of the homeowner or residents, whether the home is empty or if there are people present.[253] These historic rules show that the physical space of an individual’s home is usually considered a personal space and private to the individual.

[252] Chabad Sola – South Cienega, CA (Jewish.tv) home page Talmud, *Bava Metzia* 113, 8:35–49:16 <http://dot_net-origin.chabad.org/dailystudy/talmud_cdo/aid/3446486/jewish/Talmud-Bava-Metzia-113.htm>.
[253] Quran *Al-Nur*, 24:27–28 <https://quran.com/24/27-28>.

Futuristically, Daniel Joyce presents an interesting commentary with regards to the use of 'spatial' in relation to the internet. I refer to his comments allegorically regarding SMedia. While accepting that the spatial correlation is somewhat like a real estate model, Joyce suggests that viewing the internet in more holistic terms 'as an environment rather than a mechanism or extension of the public' may prove more constructive, as the internet is a more than a conceptualisation of a new world or a 'binary conception of online/offline' realm.[254] In light of the pervasiveness of SMedia (as discussed in Part 1), the word 'environment' seems to encapsulate the notion that is SMedia today. However, the above definition of spatial privacy is maintained for the purposes of this thesis. Joyce's idea is too abstract for this paper and may open a broad area of debate and discourse too wide for this space.

2.1.2. Personal privacy

2.1.2.1. Privacy of person (bodily privacy)

Historically, notions of personal privacy can be traced to the Bible, Quran and other ancient texts. One example of personal privacy is exemplified in the book of Genesis when Adam and Eve are expelled from the Garden of Eden after being made conscious of their 'shame' from the nakedness of their bodies.[255] This was an

[254] Daniel Joyce, 'Privacy in the Digital Era: Human Rights Online?' (2015) 16(1) *Melbourne Journal of International Law* 270, 6. Daniel Joyce is a lecturer at the School of Law, University of New South Wales, Project Director of the Digital Media and Human Rights, Australian Human Rights Centre and an Affiliated Research Fellow at the Erik Castren Institute of International Law and Human Rights, University of Helsinki.
[255] Henry F Fradella et al, 'Quantifying Katz: Empirically Measuring "Reasonableness Expectations of Privacy" in the Fourth Amendment Context' (2011) 38(3) *American Journal of Criminal Law* 289, 299.

awareness of exposure, of their nakedness being disclosed to the world around them.[256]

The *Mahabharata* is another example from an ancient civilisation in which personal privacy is evidenced. The *Mahabharata* is an Indian legend passed down through oral tradition and reputed to be about 5000 years old.[257] In this legend, an example of personal privacy is expressed in the non-criminal circumstance of the protagonist Draupadi's experience of being humiliated when the villain Dhusasana pulls at the garments she is wearing and the way in which the hero Krishna saves her modesty.[258] In this context, Draupadi's unwillingness to expose her body to eyes other than those whom she permitted to view her body may be said to be a personal right of bodily privacy. Another example is the Biblical sixth commandment that prohibits adultery.[259] This example suggests that the body of a married person belongs to the spouse and that bodily privacy is an exclusive property right rather than a personal right.[260] These two examples may be taken to indicate that an individual's privacy in relation to their (human) body overlaps between spatial privacy (property) and personal privacy.

This overlap is relevant when discussing the images of people posted on personal SMedia sites. One contemporary example is when an incensed third party posted a screenshot of a video. The video was uploaded by two naval nurses in the US. It

---

[256] Kenneth Mathews, *The New American Commentary: Genesis 1-11:26 (New American Commentary)* (B & H Publishing Group, 1996) 26.
[257] The *Mahabharata* is originally attributed to Vyasa and has been translated by various people in multiple languages including English.
[258] Kamala Subramaniam, *Mahabharata* (Bhavan's Book University, 19th ed, 2015) 192–3.
[259] Henry F Fradella et al, above n 254, 289, 301, citing Arnold N Enker, 'Error Juris in Jewish Criminal Law' (1994–1995) 11 *Journal of Law and Religion* 23, 42.
[260] Henry F Fradella et al, above n 254, 289, 301, citing Jill Elaine Hasday, 'Contest and Consent: A Legal History of Marital Rape' (2000) 88(5) *California Law Review* 1373, 1397 n 68.

showed the nurses making a newborn infant dance to rap music.[261] The third party shared the images posted by one of the nurses outside the SMedia site of the person posting the image. Could it be argued that the third party had no right to 'share' the screenshot of the video that was presumably posted for the select audience of the person (nurse) on her personal SMedia site? In this instance, it is expected that the nurses will face both military (criminal) and legal (civil) repercussions.[262] The expected repercussions for the two nurses may indicate that a posting on a personal SMedia site is tantamount to a story in the public media. The question of whether an employee's comments on personal SMedia are made on a public or private space is detailed below**.**

2.1.2.2. Privacy and secrecy

Does privacy mean secrecy? This is a question that has existed since ancient times. For example, in the Chinese legend *Butterfly Lovers* issues that relate to personal privacy and secrecy are central to the theme of the female protagonist pretending to be a man.[263] In the legend, the female protagonist dresses as a man to obtain an education in an era when it was unlawful for women to study or to be scholarly. Thus, she had to keep her gender a secret. To keep this secret (information about her person), she had to protect her personal privacy of identity, body, clothing and behaviour. This intersection between privacy (personal and spatial) and secrets is

[261] 9News, '*Nurses Removed From Duty After Making Newborn Dance for Video'* (20 September 2017) <http://www.9news.com.au/world/2017/09/20/07/54/nurses-removed-from-duty-after-making-newborn-dance-for-video>.
[262] Ibid.
[263] Victor Mair, 'An Eighteenth-Century Version of "Liand Shanbo and Zhu Yingtai" from Suzhou' in Victor Mair (ed), *The Columbia Anthology of Chinese Folk and Popular Literature* (Columbia University Press, 2011) 503.

well discussed by Bier.[264] Bier considers this intersection of maintaining privacy to support maintaining secrecy as the beginnings of legal privacy in the 20th century.[265] Bier goes on to quote Warren and Brandis's simplistic concept of privacy as 'the right to be left alone'.[266]

Des Butler, Professor of Law at the Queensland University of Technology, states that case law has firmly recognised that information 'with the requisite quality of confidence' includes secrets, whether they be trade secrets or personal secrets.[267] However, information that is made public is no longer a secret.[268] In *Wilson v Ferguson* [2015] WASC 15 a spurned lover uploaded to the internet intimate pictures of his ex-fiancée. The court commented that pictures, 'implicitly provided on condition that they were not to be shown in public', were made public when they entered a domain in which others could access them and the secret was then exposed.[269] This intersection between secrecy and privacy is a relevant consideration. This is particularly the case in relation to determining if an employee breaches confidentiality of employer information when the employee posts their opinion on SMedia.[270]

[264] William Christian Bier, *Privacy, A Vanishing Value?* (Fordham University Press, 1980), citing Samuel Warran and Louis Brandeis 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193, 195.
[265] Ibid.
[266] Ibid.
[267] Des Butler, 'Protecting Personal Privacy in Australia: Quo Vadis?' (2016) 42(1) *Australian Bar Review* 116.
[268] *Wilson v Ferguson* [2015] WASC 15.
[269] Ibid [56].
[270] Butler, above n 266.

2.1.2.3. Informational privacy

Informational privacy is the area of privacy most commonly discussed in relation to SMedia privacy. An example of informational privacy in Ancient Greece is the Hippocratic Oath that is still in use today. Through the Oath, doctors swear to protect patient confidentiality.[271] The Oath includes the words:

> What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about.[272]

As far back 1769, there is common law authority to state that it is the sole right of the maker of a statement to determine if he wants to share or publish a personal comment, opinion or any visual depiction of the same, including images and pictures.[273] Warren and Brandis' 1890 treatise on privacy expands personal privacy violations to include any information that is exploited through media, specifically print media.[274] The sentiments in their treatise echo through time and are relevant to the realm of SMedia today. Their treatise holds relevance to the issue of safeguarding the privacy and rights of an individual to communicate their thoughts and actions on SMedia.

---

[271] John C Moskop et al, 'From Hippocrates to HIPAA: Privacy and Confidentiality in Emergency Medicine Part I: Conceptual, Moral, and Legal Foundations' (2005) 45(1) *Annals of Emergency Medicine* 59.
[272] 'Oath of Hippocrates' in Warren Thomas Reich, *Encyclopaedia of Bioethics* (Macmillan, rev. ed 1995) vol 5, 2632.
[273] *Millar v Taylor* (1769) 98 ER 201.
[274] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4(5) *Harvard Law Review* 193.

In the Australian context, the importance of an individual's rights to control what is posted about an individual or entity on SMedia is underlined by the Commonwealth government's ongoing initiative to impose civil penalties on people who take, share or threaten to share nude images without consent.[275] The proposed legislation will empower the Office of the eSafety Commissioner to administer and enforce civil penalties such as fines, injunctions and orders to 'take down' (remove) such images.[276] This legislation is targeted to overarch the existing, fragmented state legislation and provide equality across all Australian jurisdictions. At present, the only states that have specific offences for such actions are New South Wales,[277] South Australia[278] and Victoria.[279] One of the ways in which the legislation aims to assist in protecting the privacy of victims, is by speeding up the process to remove such pictures from circulation. It will be interesting to see how the proposed legislation discusses sharing of such images, and whether a more extended reading of the legislation may render people who view and go on to share such posts as accountable in any way.[280]

The context of personal privacy in this thesis refers to the privacy of an employee with regards to an individual's personal information (ie, information about

[275] Angela Lavoipierre, 'National Revenge Porn Legislation to Impose Fines for Abusers Slated for This Year' *ABC News*, 10 November 2017 <http://www.abc.net.au/news/2017-11-10/new-revenge-porn-legislation-to-impose-civil-penalties/9138040>.
[276] Ibid.
[277] *The Crimes Act 1900* (NSW), amended by *Crimes Amendment (Intimate Images) Act 2017* (NSW).
[278] *Summary Offences (Filming and Sexting Offences) Amendment* Act *2016* (SA).
[279] Section 41DA of the *Summary Offences Act 1966* (Vic) that deals with the distribution of intimate images.
[280] Such sharing by third parties could and should be limited in circumstances. For example, when an individual has, or ought to have, reasonable knowledge that the original post constituted a breach of privacy, then any sharing should render the individual accountable for increasing the enormity or severity of the breach. Such accountability need not be subject to harsh punishments but rather emphasise that people should have respect for individual privacy and encourage a culture of consent and respect in SMedia.

themselves). Captured within this concept are the data, images, words, conduct and so forth that a person would consider confidential to them and those they choose to share these with. For the purposes of this thesis, personal privacy includes any information that identifies or causes an individual to be identified and information that neither an employer nor an employee may want published to any third party. This broadly follows the definition in the *Privacy Act 1988* (Cth). The *Privacy Act 1988* specifically defines 'personal information' as:

- information or an opinion about an identified individual or an individual who is reasonably identifiable a) whether the information or opinion is true or not and b) whether the information or opinion is recorded in a material form or not.[281]

It should be noted that s 6(1) of the *Privacy Act 1988* has an addendum to the definition of personal information, wherein the meaning of personal information is extended by s 187LA of the *Telecommunications (Interception and Access) Act 1979* (Cth) to cover information that is stored pursuant to Part 5–1A of that *Act*.[282] In practice this means that the *Telecommunications (Interception and Access) Act 1979* (Cth), prohibits unauthorised access to, or interceptions of, stored telecommunication information except in limited circumstances.[283]

The courts have elaborated on the meaning of personal information as it applies to such information stored under the *Telecommunications (Interception and Access)*

[281] Section 6(1) of the *Privacy Act 1988* (Cth).
[282] *Telecommunications (Interception and Access) Act 1979* (Cth) (as amended by the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth)).
[283] *Telecommunications (Interception and Access) Act 1979* (Cth), see long title of the Act.

Act 1979 (Cth). For example, in *Privacy Commissioner v Telstra Corporation Ltd* [2017] FCAFC 4,[284] an individual (Grubb) requested his telecommunication provider Telstra provide him with 'all the metadata information' that it had stored about him in his mobile phone service.[285] He then filed a complaint with the OAIC,[286] alleging that Telstra had not provided him with all his personal information as requested. The Court determined that 'metadata' was not defined in the Act.[287] The Court determined the issue by a narrow interpretation of the meaning of 'personal information' of the individual.[288] The Court held that 'personal information' within the *Telecommunications (Interception and Access) Act 1979* (Cth) only included information that may become known to third parties.[289]

In information technology and information systems, metadata is defined as an underlying layer of data that describes other data. For example, a text document's metadata contains information about the length of the document, author, when the document was written and, often, a short summary of the document.[290] Metadata makes finding and working with primary data easier as it operates more like a tool than a primary source of information such as a library catalogue.[291] As a tool, metadata is deemed to be part of the intellectual property of the information technology system of the service provider rather than raw information. Thus, metadata or information contained therein is not disclosed to third parties as it is not

[284] *Privacy Commissioner v Telstra Corporation Ltd* [2017] FCAFC 4.
[285] *Privacy Commissioner v Telstra Corporation Ltd* [2017] FCAFC 4 [6].
[286] Previously known as the Office of the Australian Privacy Commissioner (OAPC).
[287] *Privacy Commissioner v Telstra Corporation Ltd* [2017] FCAFC 4 [6].
[288] *Privacy Commissioner v Telstra Corporation Ltd* [2017] FCAFC 4 [3].
[289] Ibid.
[290] P Christensson, 'Metadata' (2006) *TechTerms* <https://techterms.com/definition/metadata>.
[291] Margaret Rouse, *Metadata* (July 2014) TechTarget <http://whatis.techtarget.com/definition/metadata>.

considered relevant.[292] On the facts of *Privacy Commissioner v Telstra Corporation Ltd*, the metadata requested by Grubb was deemed not to be 'personal information' about Grubb.[293]

It should be noted that this interpretation of personal information was construed narrowly in the light of Principle 6 of the *NPPs*. The Court determined that Principle 6 was enacted to 'ensure that a person has access to information held by a relevant entity, information may become known to third parties'.[294] If *Privacy Commissioner v Telstra Corporation Ltd* were to be filed today, the relevant *APP* would be Principle 12.1 that provides guidelines about the access of an individual to their personal information.[295] However, Flannery, an Australian legal practitioner, commented that the decision in *Privacy Commissioner v Telstra Corporation Ltd* has acknowledged that 'personal information' is a 'broad concept' that requires a case-by-case evaluation to determine if information or opinion is about a particular individual or not.[296]

This thesis submits that the narrow interpretation in *Privacy Commissioner v Telstra Corporation Ltd* is the Court's attempt to balance the protection of individual personal privacy with the economics of data management in relation to business entities. Businesses would have to safeguard their corporate intelligence, customised

---

[292] *Privacy Commissioner v Telstra Corporation Ltd* [2017] FCAFC 4.
[293] Angela Flannery, 'Grubb's Case and the Meaning of Personal Information' (3 March 2017) Mondaq <http://www.mondaq.com/australia/x/573252/Data+Protection+Privacy/Grubbs+case+and+the+meaning+of+personal+information>.
[294] *Privacy Commissioner v Telstra Corporation Ltd* [2017] FCAFC 4.
[295] Office of the Information Commissioner, *Chapter 1: APP 12.1—Open and Transparent Management of Personal Information* (February 2014) <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-1-app-1-open-and-transparent-management-of-personal-information>.
[296] Flannery, above n 292.

equipment and technology and moderate their transactional costs of safeguarding against cyberthreats and increased compliance with security regulations. This interpretation is broader than that suggested by the ALRC.[297] The ALRC's *Serious Invasions of Privacy in the Digital Era* report suggests that privacy of the individual need only give way to the public interest.[298] In the report, the ALRC recommends that the criteria for 'public interest' includes 'freedom of expression, freedom of the media, public health and safety and national security'.[299]

The above submission is supported by the view of Peter Leonard, a practitioner and a director of the International Association of Privacy Professionals ANZ (iappNZ).[300] Leonard states that Principle 1 (privacy policy) and Principle 5 (obligations to notify upon collection of personal information) of the *APPs* set the tone for the main changes brought about by the *APPs*.[301] Leonard's view is that the Information Commissioner's role will develop to determine if corporate entities are implementing the legislative safeguards in relation to informational privacy.[302] Such implementation requires that corporate entities that deal with informational data will have to move beyond merely setting up policies towards ensuring that relevant processes and procedures are in place to implement said policies.[303] This thesis submits that such compliance requirements would require corporate entities and

[297] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report No 123 (2014).
[298] Ibid 143 [9.2]–[9.3]
[299] Ibid 143 [9.4].
[300] Peter Leonard, 'An Overview of Privacy Law in Australia: Part 1' (2014) 33(1) *Communication Law Bulletin* 1.
[301] Ibid.
[302] Ibid.
[303] Ibid.

employers to balance the economies of scale to invest in appropriate mechanisms to comply with privacy regulations.

As compliance with privacy protections increase, the courts may take into consideration the economies of scale (costs of compliance protections) with a narrower or more considered definition of what is required to be protected (personal information). This is to be fair to employers and corporate entities that need to safeguard their business intelligence (eg, computing systems or intellectual property) that also require protection from exposure. Importantly, the protection of corporate entities and their interests in performing their activities forms part of the *Act*.[304] Further, the ubiquitous nature of information technology, information systems, information management and information architecture has had an effect on the evolving nature of privacy as a concept in contemporary society.[305] Arguably, any judicial decisions may involve a meaningful discussion on the understanding of contemporary views regarding privacy. Such a discussion is far broader than the scope of this thesis.

[304] Section 2A(b) of the *Privacy Act 1988* (Cth).

[305] See Gry Hasselbalch Lapenta and Rikke Frank Jørgensen, 'Youth, Privacy and Online Media: Framing the Right to Privacy in Public Policy-Making' (2015) 20(3) *First Monday* <http://firstmonday.org/ojs/index.php/fm/article/view/5568/4373>. Although the number of students surveyed is small, the discussion and experiences in this article resonate with my informal findings and discussions with my own students. These students are future consumers, users and arbiters of online privacy in the not-too-distant future and their perceptions of privacy and standards of privacy are what we should be considering when discussing the future of SMedia privacy. Another interesting comment on the possible evolution of SMedia privacy is Mark Zuckerberg's public letter *Building Global Community* (17 February 2017) Facebook <https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10154544292806634>.

2.2. The Australian Position on Employee Privacy

The next relevant area of privacy is the Australian framework of privacy protections, particularly in relation to employees. This section provides a brief overview, as much of this content is considered elsewhere throughout this paper.

An employee's right to privacy as a specific concept is not protected by the *Australian Constitution* or common law.[306] However, the current Australian legal framework does afford an individual privacy rights through a range of legislative and common law safeguards.[307] The following provides an overview of these safeguards. This section is broad, although this thesis has a narrow focus on the relevant legislation and common law principles during the discussion of the unfair dismissal cases. If relevant, such discussion is specifically in relation to employee use of SMedia. In some instances, it may include a discussion of cases that may be regarded as relevant analogies to the context of employees using SMedia.

2.2.1. Overview of Australian privacy legislation

The primary piece of legislation dealing with protecting personal information in Australia is the *Act* that, together with the *APPs*, attempts to craft a regulatory framework that is overarching and consistent across Australia. These have been referred to in Part 1. The 13 *APPs* were established by Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) that amends the *Act*. The *APPs* serve to emphasise that 'personal information' as provided by the *Act*

[306] Leonard, above n 299, 1, 4.
[307] Ibid.

should be safeguarded. These are not discussed separately, but instead form part of the overarching discussion of case law when contextually relevant to this thesis.

A recent step towards embracing a more secure stance in relation to privacy of personal information in the age of digital information technology, is the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) (the *Data Breaches Act*) that will take effect on 22 February 2018.[308] The *Data Breaches Act* places a responsibility on corporate entities that store or possess personal information, including employers, to notify the OAIC if there has been, or is likely to be, a breach of personal information that does, or is likely to, cause serious harm to the said individuals.[309] There is no definition of 'serious harm' in the *Data Breaches Act.* However, the Explanatory Memorandum provides some guidance.[310] It states that 'serious harm' could include 'serious physical, psychological, emotional, economic and financial harm' as well as 'as serious harm to reputation and other forms of serious harm that a reasonable person in the entity's position would identify as a possible outcome of the data breach'.[311]

However, as Selvadurai et al note, the Explanatory Memorandum states that mere distress over unauthorised disclosure of personal information will not constitute serious harm.[312] The *Data Breaches Act* is specific in that it relates to exposure of employee, customers and other related persons' personal information from an

[308] Nick Abrahams and Jamie Griffin, 'Privacy Law: The End of a Long Road: Mandatory Data Breach Notification Becomes Law' (2017) 32 *LSJ: Law Society of NSW Journal* 76.
[309] Niloufer Selvadurai, Nazzal Kisswani and Yaser Khalaileh, 'Strengthening Data Privacy: The Obligation of Organisations to Notify Affected Individuals of Data Breaches' (2017) *International Review of Law, Computers & Technology* 1 [4.2.2].
[310] Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016 [9].
[311] Ibid n 50.
[312] Ibid n 49.

entity's database whereby the entity itself must be one that falls within the purview of the *Data Breaches Act.* For companies that collect and store data, it raises issues of more, and potentially stricter, regulatory compliance requirements, increased cybersecurity costs and possible privacy-related legal actions resulting from data breaches.[313]

The *Data Breaches Act* does not address potential threats to individuals in relation to personal information that may be available to third parties. An example of this is any information in the public domain that is easily discoverable by third parties who perform a simple internet search or phone directory search.[314] Some examples of such information include an individual's name, change of name (if any) by deed poll, postal address (that may be an individual's residential address) and details of an individual's profession or business.[315] Other information that is outside the scope of the *Data Breaches Act* may relate to the financial standing of an individual such as being declared bankrupt, stating any unclaimed monies that are owed, the value of a residential house, an official valuation, rates charged and so forth.[316] The availability of such information can lead to a general idea of an individual's financial worth. This has implications to the individual in relation to various areas such as being targeted for unwanted marketing, scams (eg, identity theft and credit card fraud) and perhaps even becoming a target for kidnapping.

[313] Abrahams and Griffin, above n 307.
[314] Judith Bannister, 'The Public/Private Divide: Personal Information in the Public Domain' (2002) 8(8) *Privacy Law and Privacy Reporter* 157.
[315] Ibid.
[316] Ibid.

From an opposing and more commercial perspective, Bannister examines the needs of businesses operating in an environment of e-commerce, the anonymity of emails and the competing interests of balancing personal privacy with the requirement for businesses who want to verify the identities of prospective clients when sourcing for clientele.[317] Bannister argues that, in Australia, personal information is private or confidential when it is information that is 'not generally known' and hence, is protected by the various privacy laws of Australia.[318] However, once such information is available to the public, it no longer receives the same extent of legal protection.[319] Bannister's argument appears to support the view that an SMedia account is a public domain.

Other legislation regulating privacy issues in Australia include the plethora of national anti-discrimination legislation such as the *Age Discrimination Act 2004* (Cth), *Australian Human Rights Commission Act 1986* (Cth), *Disability Discrimination Act 1992* (Cth), *Racial Discrimination Act 1975* (Cth) and the *Sex Discrimination Act 1984* (Cth).[320] This collection of legislation attempts to protect individuals from discrimination by making it an offence for them to be treated in a manner different from anyone else in any particular situation. These legislative protections are a separate protection from workplace discrimination. Workplace laws have their own additional and specific provisions to prevent discriminatory behaviour in the workplace. This is discussed below, together with the common law duty of an

[317] Ibid.
[318] Ibid.
[319] Ibid.
[320] Australian Human Rights Commission, *A Quick Guide to Australian Discrimination Laws* (October 2016) <https://www.humanrights.gov.au/employers/good-practice-good-business-factsheets/quick-guide-australian-discrimination-laws>.

employer to provide a safe workplace.[321] This legislation also protects the privacy of an individual, as shown by the overall aim of such legislation to prevent discrimination against, or unfair treatment of, an individual in any situation. This includes protection against unfair treatment in the workplace based on the individual's age, gender, gender identity and so forth.

This legislation only prohibits a party from acting unfairly against an individual based on any personal information of which they may have knowledge. It does not necessarily prohibit or protect personal information from being disclosed to a third party. Protection against disclosure only comes from the *Act* and any specific law requiring disclosure (eg, anti-terrorism legislation) or when the information is accessed under some other law (eg, with a warrant to investigate an offence under criminal law or national security). It is the same with regards to employees governed under the *Fair Work Act 2009* (Cth). Another area of legislative protections designed to regulate access to personal information is the collection of Freedom of Information legislation that is enacted at both Commonwealth and state levels.[322] A limited right of protection is provided to 'information related to personal affairs' being released from government records.[323] The definition of personal information in this framework is akin to 'data' as discussed above.

[321] Sections 352 and 772 of the *Fair Work Act 2009* (Cth).
[322] See, eg, the *Freedom of Information Act 1982* (Cth) and *Freedom of Information Amendment (Reform) Act 2010* (Cth), the primary amendment to reduce costs of freedom of information applications.
[323] *Colakovski v Australian Telecommunications Corporation* (1991) 100 ALR 111.

2.2.2. Overview of Australian employer–employee privacy common law duties

2.2.2.1. Employer duties

As stated earlier, the common law in relation to workplace law does not provide any clear duties for an employer to protect an employee's personal information. However, the employer does owe a duty to employees to provide a safe workplace. This duty would include protecting an employee from discriminatory behaviour through bullying or harassment in the workplace.[324] Workplace bullying costs the Australian economy an estimated $6 billion annually.[325] The increased use of information communication technologies in the workplace has contributed to cyberbullying.[326] This common law duty against bullying may be said to incorporated or received additional legislative protections under the *Fair Work Act 2009* (Cth).[327]

At present, and in the absence of specific workplace-related cyberbullying legislation in Australia, cyberbullying in the workplace is still under the purview of the *Fair Work Act 2009* (Cth).[328] With regards to employee privacy the *Fair Work Act 2009* (Cth) defines bullying as occurring when an employee is repeatedly subjected to unreasonable treatment by someone or a group of people within a workplace *and* which creates a risk to the health and safety of the discriminated employee.[329] Brown and Dent note that, in the case of *Ms SB* [2014] FWC 2104, the FWC determined 'a

[324] Section 789FD of the *Fair Work Act 2009* (Cth).
[325] Anne O'Rourke and Sarah Kathryn Antioch, 'Workplace Bullying Laws in Australia — Placebo or Panacea' (2016) 45(1) *Common Law World Review* 3, 3.
[326] Ivana Vranjes et al, 'When Workplace Bullying Goes Online: Construction and Validation of the Inventory of Cyberbullying Act at Work (ICA-W)' (2017) *European Journal of Work and Organizational Psychology* 1.
[327] Section 789FD of the *Fair Work Act 2009* (Cth).
[328] Section 789FD of the *Fair Work Act 2009* (Cth).
[329] Section 789FD of the *Fair Work Act 2009* (Cth).

reasonable management action' would not constitute 'bullying'.[330] An example of a reasonable management decision is *Tao Sun* [2014] FWC 3839, in which the FWC held that an employer who had instructed an employee to do work that was not in their job description was not guilty of bullying the employee.[331] Brown and Dent also observe that the legislative provisos do not protect all employees.[332] They only protect employees who work in entities that are covered by the *Fair Work Act 2009* (Cth).[333] The *Fair Work Act 2009* (Cth) also provides that an allegation of discrimination must be evidenced by repetitive behaviour.[334] Arguably, any ongoing surveillance of an employee's SMedia accounts may fulfil this requirement of repeated behaviour.[335]

An example of bullying via SMedia is *Application by Roberts 1* [2015] FWC 6556. In this case, the FWC ruled that 'unfriending' an employee or co-worker amounted to bullying.[336] On the facts of this case, there was a series of incidents between Mrs Bird, the supervisor, and Ms Roberts, the plaintiff.[337] One incident that happened towards the end of their working relationship was the action of Mrs Bird, who deleted Ms Roberts as a friend from her Facebook page a few minutes after a particularly fractious altercation between the two.[338] Wells DP characterised the action of

[330] Murray Brown and Chris Dent, 'Employer Access to Employee Social Media — Privacy and Regulations' (2017) 43(3) *Monash Law Review* (forthcoming) 21; *Ms SB* [2014] FWC 2104.
[331] *Tao Sun* [2014] FWC 3839.
[332] Brown and Dent, above n 329.
[333] Brown and Dent, above n 329; s 789FD(3) of the *Fair Work Act 2009* (Cth) and *Re Ms SW* [2014] FWC 3288.
[334] Section 789D(1)(b) of the *Fair Work Act 2009* (Cth).
[335] Brown and Dent, above n 329.
[336] *Application by Roberts 1* [2015] FWC 6556 [89].
[337] Ibid [3].
[338] Ibid [87].

'defriending' as one that 'evinces a lack of emotional maturity and is indicative of unreasonable behaviour'.[339]

2.2.2.2. Employee duties in relation to employer privacy

From an employee's perspective, the common law clearly states that employees owe several duties to protect their employer's privacy. The question is, are these duties, or possible breaches of them, relevant considerations that the court may take into account in determining whether an employer has any rights to access or request access to an employee's SMedia site? There are four common law duties for employees that are relevant to this discussion. These duties are: the duty of care and competence, the duty to protect, the duty of fidelity and the duty to obey.

The duties in relation to an employee's duty of care and competence and duty to protect the employer's property are not usually directly relevant to this thesis. This is because these duties usually operate in relation to employee conduct and employee activities on employer-built SMedia sites. Such sites are often created by the employer for marketing outreach, brand building, customer relationship purposes or as an enhanced avenue for customer service.

An employee's duty of care and competence is an implied warranty to exercise reasonable care at work.[340] It is an established duty and extends to all employees, not just professionals.[341] In the context of this thesis, the former may broadly defined as an employee's duty to use reasonable care and competence in relation to posts

[339] Ibid [89].
[340] *Harmer v Cornelius* (1858) 5 CNBC 236.
[341] Ibid 246.

made on the employer's SMedia sites.[342] For example, I would theorise that whoever was in charge of the Russian Coca-Cola advertising campaign would not have held on to their position after making the following mishap. In this instance, a Coca-Cola campaign in Russia showed an inaccurate map of Russia. This led to a backlash by Russian consumers who then posted Facebook posts of Coca-Cola being flushed down the toilet.[343] A simple error in geography unrelated to the actual product led to an unexpected and unprecedented adverse repercussion to the brand. The real-time accountability to use due care and competence when utilising SMedia may be said to be of a higher standard than in previous, perhaps more forgiving, consumer eras.

The latter duty is an extension of the former.[344] When an employer gives an employee a task, they place their property within the control of the employee who is expected to take reasonable care of that property.[345] Arguably, this duty can be amplified to include employee posts on employer-related SMedia activities that result in the employer's reputation being damaged. One example is when MTV Australia posted an offensive tweet asking for English subtitles when Eva Longoria and America Ferrera, both actresses of Mexican decent, were onstage during the Golden Globe awards.[346] Neither of these examples are directly relevant to employee posts on their personal SMedia sites that result in dismissals and is the focus of this thesis.

[342] Lindsay Friedman, *The 12 Worst Social-Media Fails of 2016* (22 September 2016) Entrepreneur <https://www.entrepreneur.com/slideshow/272286#0>.
[343] Ibid.
[344] Natalie van der Waarden, *Understanding Employment Law: Concepts and Cases* (LexisNexis Butterworths, 3rd ed, 2014) 122 [6.11].
[345] Ibid; *Lister v Romford Ice and Cold Storage Co Ltd* [1957] AC 555.
[346] Friedman, above n 341. In this instance, the apparent racism lead to the tweet being considered extraordinarily offensive.

Employee duties that are more commonly construed as being directly relevant to protecting an employer's privacy are the duties of fidelity and obedience. It is an established common law principle that an employee owes an employer the duty of fidelity.[347] This implies a duty to safeguard the employer's reputation.[348] For instance, an employee must act in a manner befitting the scope of employment when not to do so may injure the employer's reputation. Such injury may result in an adverse reaction from the employer's customer base. One example is the case of Justine Sacco, previously the director of communications at media company IAC. At the time, IAC also owned online dating site Tinder and the *Daily Beast* (an American news and opinion website focused on politics and pop culture). Sacco was sacked soon after she tweeted 'Going to Africa. Hope I don't get AIDS. Just kidding. I'm white!'.[349]

The duty of fidelity also includes the duty to maintain the confidentiality of any information related to an employer's work, processes and other aspects that may impinge adversely on the employer if disclosed.[350] This duty may be said to incorporate an employee's duty to report the misconduct of others. Some of the unfair dismissals discussed are a result of a person other than the dismissed employee (ie, either a co-worker or a superior) reporting to their management the employee's posts on their personal SMedia.[351] The Victorian Supreme Court has

[347] *Blyth Chemicals v Bushnell* (1933) 49 CLR 66, 81–82.
[348] *Orr v University of Tasmania* (1957) 100 CLR 526.
[349] Carolyn Sun, *These Social Media Fails Got People Fired* (18 March 2016) Entrepreneur <https://www.entrepreneur.com/article/271823>. Note the example of Justine Sacco who tweeted about getting AIDS before flying to Africa.
[350] *Faccenda Chicken Ltd v Fowler* [1986] 1 All ER 617, 625–8.
[351] *Linfox Australia Pty Ltd v Stutsel* [2012] FWAFB 7097 [2]. In this instance, a manager accessed the Facebook page of an employee and reported what she saw to management, leading to the alleged unfair dismissal of the employee.

ruled that there is no such employee duty at common law (nor statute).[352] In *Hodgson v Amcor* [2012] VSC 94, Vickery J held that employees are under no general duty to report fellow employees' misconduct. Exceptions to this may arise when it is required by an express term in a contract of service, or by virtue of an employee's position such as supervisory levels, who may be required to report misconduct of people under their supervision as not to do so may breach the supervisor's duty to act in the best interest of their employer.[353]

Another common law duty that an employee owes to the employer is the duty to obey lawful and reasonable orders. This duty is discussed particularly in relation to an employee's knowledge of, acceptance and obedience to, an employer's workplace and SMedia policies in Part 3 of this thesis. Part 3 discusses the central issue of this thesis — how the Australian courts view disgruntled employees who are dismissed as a result of complaining about or posting about their co-workers, workplace, jobs or supervisors on the employees' personal SMedia sites. Part 3 brings together some of the issues previously discussed such as employee duties, privacy and the specific context of an employee's posts on their personal SMedia sites that result in their dismissal.

[352] *Hodgson v Amcor* [2012] VSC 94 [1575]–[1576], cited by Dan Trindale, 'Employees' Duty to Report Misconduct of Themselves or Others' on Clayton Utz, *Knowledge* (26 April 2012) <https://www.claytonutz.com/knowledge/2012/april/employees-duty-to-report-misconduct-of-themselves-or-others>.
[353] Ibid.

Part 3: Employee Privacy on SMedia

There are three interrelated areas of discussion for this part of the thesis. First, a discussion to determine the scope and ambit of an employee's rights to privacy when using SMedia. This will include whether SMedia is considered to be a public or private space. More particularly, this portion of the thesis will explore what rights, if any, employees have in the realm of SMedia to protect their private communications about their job, colleagues or employer. This discussion will canvas all SMedia media activities including communications made to friends and family through posts, pictures, comments, likes and so forth. Several seemingly disparate issues will be examined including employer control of employees' after-work activities, political freedom of speech, the means by which the information was obtained by the employer, characteristics of the employee (eg, length of service, age and digital literacy) and the possibility of obtaining another position.

The second area of discussion will involve determining the scope, if any, of the duties that employees owe their employer that may act to restrain the employee's 'freedom' of speech when communicating through SMedia opinions about their work, employer or any other work-related matter. This discussion will continue from the common law duties discussed earlier.

The third area for discussion flows from the first two areas and involves determining the rights, if any, that employers have to restrain or oversee their employee's personal SMedia communication.

A discussion of these three areas involves a review of relevant court decisions. This is required to determine if there is a trend in judicial decision-making related to unfair dismissals, employees and their use of personal SMedia. First, a brief overview is provided of the law that surrounds the termination of employees due to perceived wrongdoings. This overview provides the context for the later discussion. The overview supplements material that has been discussed in Part 1 of this thesis as part of the discussion of contemporary workplace and employee privacy. The overview will also provide an appreciation for the legal principles used by the courts in delivering their judgments.

3.1. Termination of Employment in Australia

3.1.1. *Fair Work Act 2009* (Cth)

Most employment relationships are governed by contracts of service that provide for agreed termination and for situational breaches of contract. However, the types of termination discussed in this paper primarily involve terminations under the *Fair Work Act 2009* (Cth) (*Fair Work Act)*. For example, consider the situation of an employee who is dismissed for posting on their personal SMedia site a comment or picture to which the employer takes offence.[354] Whether such a dismissal is valid is the purview of the judicial system based on the law as stated in the *Fair Work Act*.[355] The adjudication system under the *Fair Work Act* begins with decisions from the FWC. Those decisions can, in certain circumstances (including by way of leave from

[354] *Smith v Fitzgerald* [2011] FWAFB 1422 [13]–[15]. The Full Bench of the Fair Work Commission found the dismissal unfair, as it was not consistent with the Small Business Fair Dismissal Code and the employee's conduct both on and off Facebook did not warrant their dismissal.
[355] Sections 340–345 and ss 379–405 of the *Fair Work Act 2009* (Cth).

the court on an error of law or in the public interest), be appealed to the High Court. The *Fair Work Act* provides that a dismissal may be valid if it does not contravene the unfair dismissal[356] or general protections (adverse actions[357] and unlawful termination) provisions.[358]

3.1.2. Unfair dismissal

The *Fair Work Act* defines 'unfair dismissal' as a dismissal that is 'harsh, unjust or unreasonable'.[359] The *Fair Work Act* provides some guidance as to the criteria that may constitute 'harsh, unjust or unreasonable' that includes both situational and procedural factors. The most relevant criteria for the purposes of this paper are the situational factors that require the court to consider 'whether there was a valid reason for dismissal related to the person's capacity or conduct (including its effect on the safety and welfare of other employees)'.[360] Conduct is defined by the *Fair Work Act* to include omissions by an employee.[361]

When will the courts accept a termination as justified?

The Act presents a two-step test in which the employer must show a valid reason for the termination.[362] The employer must do this by demonstrating a nexus between the employee's conduct and their employment.[363] The courts use a common sense

[356] Sections 379–405 of the *Fair Work Act 2009* (Cth).
[357] Ibid s 342.
[358] Ibid ss 379–405.
[359] Ibid s 385(b).
[360] Ibid s 387(a).
[361] Ibid s 12 (definition of 'conduct').
[362] Ibid s 387(a).
[363] *Rose v Telstra* [1998] AIRC 1592.

approach to determine if a valid reason exists.[364] For example, Justice Moore stated that the (mis)conduct must have both occurred and be sufficiently grievous or repetitive to validate termination as a consequence.[365] The employer must satisfy the usual burden of proof 'on balance of probabilities'. However, the courts have indicated that 'the strength of the evidence necessary to establish a fact or facts on the balance of probabilities may vary according to the nature of what it is sought to prove'.[366]

The second and separate consideration that the courts will examine is whether the termination is 'harsh, unjust or unreasonable' in the circumstances of the individual case.[367] The Act provides for a variety of (non-exhaustive) factors to be considered.[368] Some factors that courts have considered include the economic situation of the employee and the consequences of termination that are personal to their particular situation in life.[369] Justices McHugh and Gummow noted that a termination will not be upheld if the court considers termination a disproportionate consequence in relation to the employee's misconduct.[370] One example is *Linfox Australia Pty Ltd v Stutsel* [2012] FWAFB 7097 in which the court took into account the employee's age and lack of knowledge in relation to the operation of his SMedia account when determining his dismissal as unfair.[371]

---

[364] *Selvachandran v Peteron Plastics Pty Ltd* (1995) 62 IR 371 [373], reg 1.07 Fair Work Regulations 2009 (Cth).
[365] *Edwards v Guidice* [1999] FCA 1836 [4] [6]–[7].
[366] *Neat Holdings Pty Ltd v Karajan Holdings Pty Ltd* (1992) HC 67 ALJR 170, per Mason CJ, Brennan, Deane and Gaudron JJ [2].
[367] Section 385 *Fair Work Act 2009* (Cth).
[368] Ibid s 387.
[369] *NSW AG Department v Miller* [2007] NSWIRComm 33 [113]–[123].
[370] *Byrne v Australian Airlines Ltd* (1995) 185 CLR 410.
[371] *Linfox Australia Pty Ltd v Stutsel* [2012] FWAFB 7097 [34].

The cases that follow illustrate that unfair dismissal is a common form of court adjudicated dismissals in relation to employees being dismissed due to their usage of SMedia.

3.1.3. Adverse action and unlawful termination

In *McIntyre v Special Broadcasting Services Corporation* [2015] FWC 6768, the Court referred to the relationship between the general protections and unlawful terminations under the *Fair Work Act*.[372] The Court referred to the Explanatory Memorandum to the Fair Work Bill 2008 (Cth) to explain that while both these employee remedies against dismissals are similar in nature, they are intended to protect different classes of people. In fact:

> the unlawful termination provisions are only intended to be an extension of these (general) protections to persons who are not covered by the general protections in relation to the termination.[373]

With this explanation in mind, the following discussion aims to set out a brief overview of the adverse action remedy. This remedy is an integral part of the general protections and unlawful termination.

3.1.3.1. Adverse action

A cause of action under adverse action is made specifically in relation to termination of employment. An employer who dismisses an employee in breach of a workplace right may face a claim for adverse action under s 342 of the *Fair Work Act.*[374] To

[372] *McIntyre v Special Broadcasting Services Corporation* [2015] FWC 6768 [38].
[373] Explanatory Memorandum, Fair Work Bill 2008 (Cth) cl 723 [2702].
[374] Section 342 of the *Fair Work Act 2009* (Cth).

succeed under a claim for adverse action, the aggrieved employee must prove the elements provided for in s 340 of the *Fair Work Act*.[375] Employees alleging adverse action must prove that they have been dismissed (ie, they have suffered adverse action) as a result of them having, using or abstaining from using a workplace right. The burden then shifts to the employer to disprove that the dismissal was not caused by the employee's exercise of their workplace right. The term 'workplace right' is broadly defined and includes rights under the *Fair Work Act* as well as rights that arise from ratified collective agreements and modern awards.[376] An employee may succeed in a claim of adverse action even if the workplace right is only one of many factors that resulted in the dismissal.[377] For example, in *CFMEU v Hail Creek Coal Pty Ltd* [2016] FCA 1032 a miner suffered a back injury while at work. When he returned to work, his injury prevented him from completing his usual duties and he was re-trained as a drill operator. While working as a drill operator, he brought an action against his employer in relation to his injury and was awarded damages on 15 November 2013. On 18 November 2013, at a pre-arranged medical assessment it was found that the miner's back injury had become worse and he was unfit to continue with his existing duties as a drill operator. The miner was immediately stood down (effectively dismissed) on 19 November 2013. The miner alleged that he was stood down, not because he was unfit to operate the rig, but because he had pursued the employer for damages arising from his back injury (a 'workplace right' that he

[375] Section 340 of the *Fair Work Act 2009* (Cth) prohibits adverse action.
[376] KPMG, *Process Review of Fair Work Australia's Investigations into the Health Services Union* (17 August 2012), Fair Work Commission <https://www.fwc.gov.au/documents/documents/organisations/reports/kpmg_review.pdf>, cited by Louise Floyd and Max Spry, 'Four Burgeoning IR issues for 2013 and Beyond: Adverse Action; Social Media & Workplace Policy; Trade Union Regulation (After the HSU Affair) and the QANTAS aftermath' (2013) 37 *Australian Bar Review* 153, 157.
[377] Section 360 of the *Fair Work Act 2009* (Cth).

was entitled to pursue). Conversely, the employer claimed that the 'primary and only' reason for their decision to stand down the miner was because the miner had failed to comply with Coal Mining Safety and Health Regulations.[378] However, the employer was unable to discharge the 'reverse onus of proof' to prove that the miner's back injury was not a reason for his dismissal. The Federal Court found that the employer's standing down of the miner was an adverse action and the employee succeeded in his action.[379]

A claim for adverse action is also available when an employee is dismissed as a result of some form of discrimination. Such an 'adverse' action may amount to a breach of the 'other protections',[380] in particular s 351 of the *Fair Work Act*. This section is to be read in conjunction with other specific anti-discrimination provisions in the *Fair Work Act* such as s 772(1)(f).[381] A claim for adverse action citing discrimination is to be treated as a remedy in addition to the various anti-discrimination legislation previously discussed in Part 1 under pre-hiring practices.[382] This means an employee who is dismissed as a result of discrimination has the option to claim adverse action under the *Fair Work Act*, s 772(1)(f) of the *Fair Work Act* or other relevant anti-discrimination legislation.

Unlawful termination occurs when employers dismiss employees in relation to actions prohibited by s 772 of the *Fair Work Act*. These include termination of

[378] Section 46 Coal Mining Safety and Health Regulations.
[379] *CFMEU v Hail Creek Coal Pty Ltd* [2016] FCA 1032 [95].
[380] Sections 351–356 of the *Fair Work Act 2009* (Cth).
[381] Ibid s 772(1)(a)–(h).
[382] Louise Floyd and Max Spry, 'Four Burgeoning IR issues for 2013 and Beyond: Adverse Action; Social Media & Workplace Policy; Trade Union Regulation (After the HSU Affair) and the QANTAS aftermath' (2013) 37 *Australian Bar Review* 153, 157.

employment due to temporary absence from work due to illness[383] or parental or maternity leave,[384] membership or non-membership of a trade union,[385] political opinions of an employee [386] and so forth.

McIntyre v Special Broadcasting Services Corporation [2015] FWC 6768 is one case of an employee who alleged his dismissal was due to unlawful termination as a result of his SMedia use.[387] The case involved an application for unlawful termination under s 772(1)(g) of the *Fair Work Act*. McIntyre was employed as a reporter with SBS.[388] He was dismissed for expressing his personal political opinions on his SMedia site. His opinions were made on ANZAC Day in relation to Australian Defence personnel.[389] The disputed issues in this case relate to jurisdictional objections and limitation of time, not specifically with regards to SMedia.[390] Unfortunately, no issue of law or fact was determined directly in relation to the alleged dismissal resulting from McIntyre's comments on his SMedia. However, the presiding Commissioner did comment, in passing, on the irony of McIntyre's comments regarding the very same class of people (ie, defence personnel) who had 'lost their lives in the earnest pursuit of the protection of rights and freedoms such as the access to a fair hearing which the applicant (McIntyre) was entitled to claim'.[391] The Commissioner's remark can be read as implying that an employee's comments on SMedia are covered by an inherent right to freedom of speech. This view is echoed clearly in *Starr v*

[383] Section 772(1)(a) of the *Fair Work Act 2009* (Cth).
[384] Ibid s 772(1)(g).
[385] Ibid s 772(1)(b),(c).
[386] Ibid s 772(1)(g).
[387] *McIntyre v Special Broadcasting Services Corporation* [2015] FWC 6768 [7].
[388] Ibid.
[389] Ibid.
[390] Ibid [43].
[391] Ibid [46].

Department of Human Services [2016] FWC 1460 and is discussed further below. The decision in *McIntyre v Special Broadcasting Services Corporation* also suggests that an employee's SMedia is personal to the owner of the SMedia account. This case is, perhaps, a singular example of an alleged unlawful termination in relation to employee comments on SMedia.[392]

3.1.4. Termination for breach of workplace policies

A separate cause of dismissals that is more affiliated with termination in relation to a breach of contract (rather than breach of legislation) involves breaches of workplace policies, in particular SMedia policies.

It is increasingly common for companies to formulate SMedia policies and internet policies that employees must abide by. These policies have emerged as a coherent body of policy-based remedy for employers to manage conflicts that arise from employee SMedia use to minimise any potential adverse effect on a company's brand or reputation.[393] The prevailing corporate view is that to prevent any conflict around defining the SMedia space as being either private or public, a SMedia policy is articulated as part of the contract of employment. Once accepted by the employee, such contractual obligations might be viewed as placing employee SMedia posts within the legal purview of the employer's Orwellian-like gaze and management. However, it should be noted that the courts have indicated an unwillingness to allow

[392] Brown and Dent, above n 329,18.
[393] Aliah D Wright, *Necessary Evil: Managing Employee Activity on Facebook, LinkedIn and the Hundreds of Other Social Media Sites* (Society for Human Resource Managers, 2013) Abstract.

employers to enforce such policies unless they comply with certain protocols, as will be discussed below.

3.1.5. Australian courts and SMedia policies

The Australian courts have struggled to balance the equities of employee privacy and professionalism when determining cases related to dismissals resulting from employees' SMedia posts. Through various decisions, the courts have indicated the importance of companies having clear, transparent and up-to-date SMedia policies. It seems the prevailing judicial view that in this digital age employers must implement a SMedia policy to clarify codes of conduct in the workplace.[394] Such policies should, insofar as is practicable, be incorporated into the contract of employment. If they are not, employees may not be penalised for comments made on SMedia.[395]

In one example, the Federal Court of Australia held that an employee who was fired for using inappropriate language to criticise his management on his personal Facebook account was unfairly dismissed.[396] In *Linfox Australia Pty Ltd v Fair Work Commission and Stutsel* [2013] FCAFC 157, the employee (Stutsel) had posted uncomplimentary remarks about his employer (Linfox) and its staff on his personal Facebook page.[397] He had also posted specific and unfavourable remarks about two of his managers.[398] His Facebook friends viewed and commented on his post.[399] Two pertinent factors in this instance were that Stutsel did not remove these

[394] *Linfox Australia Pty Ltd v Fair Work Commission and Stutsel* [2013] FCAFC 157. Note, this reference is for the lower court's judgment as the appeal did not comment on this point.
[395] Ibid.
[396] Ibid.
[397] Ibid [2].
[398] Ibid.
[399] Ibid [3].

comments and his privacy settings were not limited; therefore, anyone who had a Facebook account could view his post and his friends' comments.[400] One of his managers used her Facebook account to access Stutsel's post and subsequently made a complaint to the employer. This complaint resulted in Stutsel being dismissed for making derogatory, racially offensive and sexually discriminatory comments about his two managers.[401] The manager who complained was not a Facebook friend of Stutsel and had accessed his Facebook post on her own accord. As noted above, she could do so because Stutsel's Facebook privacy settings allowed public access to his profile.

Thornthwaite refers to the fact that the Court accepted that Stutsel was a mature age employee who may not have understood the privacy settings available to him on Facebook.[402] Thornthwaite goes on to point out Prensky's findings that such challenges of SMedia are peculiar to those born before the internet age.[403] Arguably, the courts may not be so forgiving of lax privacy settings from a younger employee. In the employer's appeal, Dowsett, Flick and Griffiths JJ upheld the Fair Work Commissioner's decision that Stutsel's dismissal was unfair. The portion relevant in relation to this discussion on SMedia policy is that, in his judgment, the Commissioner noted that Linfox had no SMedia policy in place.[404] By categorising this as a relevant factor the Commissioner, by implication, has indicated that had the employer formulated an SMedia policy to set boundaries on employee conduct, the decision may have been different. A similar notion may be imputed from *McIntyre v*

[400] *Linfox Australia Pty Ltd v Fair Work Commission and Stutsel* [2013] FCAFC 157 [3]–[4].
[401] Ibid [4]–[5].
[402] Louise Thornthwaite, 'Social Media and Work: An Emerging Privacy' (2016) 135 *Precedent* 8.
[403] Ibid, citing Marc Prensky, 'Digital Natives, Digital Immigrants' (2001) 9(5) *On the Horizon* 1.
[404] *Stutsel v Linfox Australia Pty Ltd* [2011] FWA 8444 [87].

Special Broadcasting Services Corporation, in which the employee's dismissal for his use of SMedia could have potentially been avoided by the implementation of a clear SMedia policy by the employer.[405] This is because if there had been a policy that was made known to him and fairly enforced, the employee would have been under contractual obligation not to write such things. Disobedience would be a breach of a clear contractual term, not an allegation under the *Fair Work Act* for unfair dismissal.

In *Pearson v Linfox Australia Pty Ltd* [2014] FWC 446, the FWC provided some focus areas for employers to formulate their SMedia policies.[406] The FWC provided a definitive endorsement for the applicability of SMedia policies. It stated that 'the establishment of a social media policy is clearly a legitimate exercise in acting to protect the reputation and security of a business … it also serves a useful purpose by making clear to employees what is expected of them'.[407] The employee (Pearson) was dismissed for breaching several of the employer's (Linfox's) workplace policies including a policy requiring contact with a relevant supervisor or manager when absent from work, a policy about mobile phone use, a policy concerning SMedia and the Safe Working Procedures policy.[408] In relation to the SMedia policy, Pearson had been given one-on-one training and had attended a group training session.[409]

However, this decision is not a blanket approval of the indiscriminate use of SMedia policies against employees. In another case, the majority of the Full Bench of the

[405] *McIntyre v Special Broadcasting Services Corporation* [2015] FWC 6768.
[406] *Pearson v Linfox Australia Pty Ltd* [2014] FWC 446.
[407] Ibid [46].
[408] Ibid [45], [49].
[409] Ibid [14], [45].

FWC clearly indicate that even when it is part of a contractual obligation, an employer is bound to bring a SMedia policy to the attention of the employee against whom it is seeking to enforce the policy.[410] It went on to point out that when employers are not consistent in enforcing such a policy, they may be precluded from relying on it.[411] A takeaway from the decision in *B, C and D v Australian Postal Corporation* [2013] FWCFB 6191 is that the mere proof, even if clear, of a breach of the SMedia policy does not in itself provide a definitive right to dismiss an employee, especially not to do so summarily.

In this case, three employees of Australia Post had emailed each other pornographic material in contravention of Australian Post's SMedia policy. While many employees were found embroiled in the emails, the three employees were the only ones who were dismissed, while others were warned or reprimanded. In examining the validity of the dismissals, the court viewed several factors including notice and enforcement of the SMedia policy, the employees' age, length of service, previous conduct, potential to obtain other employment and the absence of actual harm or damage suffered by Australian Post.[412] The original decision was subject to appeal. On appeal from the Full Bench, the Federal Court decided on jurisdictional issues. Additionally they considered whether there had been a failure to consider the public interest factor when the Full Bench refused an appeal by one of the appellants. These considerations were not directly related to the discussion on the existence or

[410] *B, C and D v Australian Postal Corporation* [2013] FWCFB 6191 [68].
[411] Ibid [96].
[412] Ibid [88].

enforcement of the SMedia policy.[413] Therefore, the law as discussed in the original case and approved by the Fair Work Full Bench is still valid at present.

From the discussion above, it is possible to conclude that when an employer has a transparent SMedia policy in place that is consistently and fairly enforced, the courts will hold employees bound by the policy when the employees use SMedia platforms.

3.2. Scope and Ambit of Employees' Rights to Privacy When Using SMedia

Referring to the first of three areas of discussion outlined earlier, this section will discuss the scope and ambit of an employee's rights to privacy when using SMedia. In the absence of constitutional or common law protections of privacy as a right, and the focus of legislative privacy protections leaning towards security of data and personal information, employees using SMedia are left in a state of doubt. They are left in uncertainty as to their privacy rights in relation to social commentary which may involve work related persons or grumbles on their personal SMedia sites. This leaves the judicial system as the arbiter to determine the breadth and width of the space that may be considered private within SMedia. The two main legal perspectives involved in this discussion are workplace laws and privacy principles. Both of these are, and must be, engaged to protect the rights of individual employees who are dismissed for communications on their personal SMedia accounts.[414] This is because the individual perspective of how employers and employees view

[413] *Australian Postal Corporation v D'Rozario* [2014] FCAFC 89. Note, in *B, C and D v Australian Postal Corporation* [2013] FWCFB 6191 the employees were not identified. After the employer's appeal was dismissed, the employees used their own names to continue with legal action.
[414] Brown and Dent, above n 329, 1.

communications via SMedia platforms — either as a personal communication, a privacy-related issue (employee) or as an action that warrants dismissal for breach of workplace laws or policies (employer) — is dependent on who feels disadvantaged. Unfortunately, in most situations both parties are disadvantaged and thus, a less divisive, more permeable approach to privacy and workplace laws might provide fairer outcomes for both employer and employee.[415]

Brown and Dent categorise three competing tensions surrounding the regulation of SMedia that are pertinent to the workplace relationship and the role of the employee.[416] Thornthwaite describes this as being the individual employee's standpoint to being 'entitled to a private life'.[417] This relates to the question of how courts view the space that is SMedia. Are employees' personal SMedia accounts and their communications made on a personal or public space?

3.2.1. SMedia — public or private space?

As stated earlier, despite the high level of interaction between users through posts (eg, Tweets, Facebook posts, Instagram pictures or private messaging) no direct human contact is made through eye, physical touch or voice. The reach of SMedia communication in the sense of one post or message being communicated to many people has often rendered SMedia communications being perceived as being 'public' communications to the 'world at large' rather than as private communications.[418] This also seems to be the way in which the FWC previously

[415] Ibid.
[416] Ibid.
[417] Thornthwaite above n 16,164, 170, citing *Rose v Telstra* [1998] AIRC 1592.
[418] Thornthwaite, above n 401.

viewed SMedia communication in relation to employee postings, as evidenced in several cases in which the FWC considered posts on Facebook and other SMedia platforms as being sufficient grounds for dismissal.[419] However, in more recent cases the view of Australian courts seems to be shifting from viewing SMedia as a purely public forum to one that has a clear delineation of privacy within the public space.

Wilson v Ferguson is a non–employment-related case that alludes to the online space as a public space.[420] As previously discussed in section 2.1.2.2, Ferguson had posted explicit photographs and videos of his ex-fiancée on his Facebook page.[421] These images were taken while the two individuals were in a relationship together and were subsequently posted on Ferguson's Facebook page after Wilson ended the relationship.[422] Wilson's case may be distinguished from the general employment law cases in that the court held that the parties were in a 'special relationship' that gave rise to a mutual duty of confidence that had been breached by Ferguson's actions.[423] Importantly, the Court commented that 'the images were not in a public domain in any sense prior to the defendant's publication of them'.[424] This indicates that the posting of such intimate images, even within a controlled, password-protected personal SMedia site, will be contextually deemed to be in a public place.

[419] See *Little v Credit Corp Ltd* [2013] FWC 9642; *Dover Ray v Real Insurance Pty Ltd (2010) FWA 8544,* (2010) 204 IR 399; *O'Keefe v William Muir's Pty Ltd* [2011] FWA 5311; *Mayberry v Kijani Investments Pty Ltd ATF The Dawe Investments Trust Subway Wallsend* [2011] FWA 3496.
[420] *Wilson v Ferguson* [2015] WASC 15.
[421] Ibid [5].
[422] Ibid.
[423] Ibid [4].
[424] Ibid [56].

The question that arises is whether this context would be considered differently when dealing with employment relationships. In *Vosper v Solibrooke Pty Ltd* [2016] FWC 1168, an employee (Vosper) who complained on Facebook about her treatment at work and her rights as an employee and was then dismissed was held to be unfairly dismissed.[425] The facts in relation to the Facebook posts by Vosper are that following a transfer of a business (Angie's Cake Emporium) to new owners (Solibrooke), Vosper was accused of breaching confidentiality when she used Facebook to private message the previous owner (her sister) regarding her unhappiness with the way the new owners treated her.[426] Vosper's sister then expressed her unhappiness at how Vosper was being treated by the new owner by saying 'Robyn isn't being treated very well at all' to another employee who went on to inform the owner about Vosper's communication.[427] Vosper also posted the news that she was leaving her job on Facebook, saying that she was 'finishing up at Angie's at the end of the week. Time to move on with a new focus'.[428] However, she did not resign but was terminated for not accepting the new employers' change in her working hours and the move to make her position a casual one from a part-time one. She then expressed her dissatisfaction on SMedia after which she brought an action against the employer for unfair dismissal. The allegation of unfair dismissal was upheld for many reasons. In their defence, the employer alleged that Vosper had breached confidentiality by expressing her dissatisfaction on Facebook. Commissioner Roe did not find any employee misconduct[429] and stated that employees are entitled to complain or

[425] *Vosper v Solibrooke Pty Ltd* [2016] FWC 1168 [20]. An appeal against this decision was dismissed in *Solibrooke Pty Ltd v Vosper* [2016] FWCFB 2421.
[426] Vosper v Solibrooke Pty Ltd [2016] FWC 1168 [12].
[427] Ibid [14].
[428] Ibid [19].
[429] Ibid [36].

express their opinion about their status or treatment at work to others.[430] Commissioner Roe also commented that, in the circumstances of the case, Vosper's comments did not amount to damaging the reputation of, or working against, the best interests of her employer. Her comments were viewed as being merely an unexaggerated expression of her own opinion on how she felt she was being treated.[431] Brown and Dent have put forward that 'self-expression is a key interest' of SMedia users.[432] From Vosper's case, it appears that the courts will seek to balance this 'self interest' against harm done to the employer. The FWC stated that 'An employee has the right to complain about their employment rights and their treatment at work. We do not live in a society in which employees are prohibited from discussing their employment status or their treatment at work with others'.[433] By implication, this decision could be taken to allude to an individual's communication on Facebook as being private even though it was made on SMedia.

Starr v Department of Human Services [2016] FWC 1460 is an employment law case that involves a public servant.[434] The nature of public servants' positions in dealing with the public, with the expectation of impartiality and confidentiality requirements, usually subject public servants to higher, more orthodox norms of behaviour.[435] Starr had been a public servant with Centrelink for 21 years and dealt with the public daily. Over three years, and on only two separate occasions, Starr had expressed his own albeit uncomplimentary views on SMedia platforms (ie, Sportal and Whirlpool) in

[430] Ibid [20].
[431] Ibid [2016] FWC 1168 [21].
[432] Brown and Dent, above n 329, 5.
[433] *Vosper v Solibrooke Pty Ltd* [2016] FWC 1168 [20].
[434] *Starr v Department of Human Services* [2016] FWC 1460.
[435] Thornthwaite, above n 401, 8,10.

relation to the length of time it took to process client applications, the paucity of federal budgets and the poor mental health and poverty of Centrelink clients.[436] He was dismissed for, among other things, behaviour that was inconsistent with Departmental policies and against the standards of 'professional probity' as a public service employee.[437]

The FWC acknowledged that on the facts there was a SMedia policy and a unit dedicated to maintaining the SMedia presence of the Department and that Starr was aware of and had breached that SMedia policy. However, the FWC rejected the reasons for Starr's dismissal and noted that for such dismissal to be valid it:

> would have to be construed expansively so as to confer on APS [Australian Public Service] departments a general right to discipline their employees for political speech communicated outside of working hours. I do not consider that the provisions should be so expansively construed.[438]

This decision follows the High Court of Australia's ruling that the *Australian Constitution* does imply a freedom of political communication and a common law right to freedom of expression.[439] Importantly, this decision gives hope to employees, including civil servants, that in circumstances in which they do not breach confidentiality, or are not inappropriate (in the specific context of their position and department) or offensive, they retain a right to state their opinion on their own personal SMedia sites.

---

[436] *Starr v Department of Human Services* [2016] FWC 1460 [18]–[19].
[437] Ibid [1], [39].
[438] Ibid [72].
[439] Ibid citing *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 559–62. See also Sally Walker, 'Lange v ABC: The High Court Rethinks the "Constitutionalisation" of Defamation Law' (1998) 5(1) *eLaw Journal: Murdoch University Electronic Journal of Law* 3 [17] <http://www.austlii.edu.au/au/journals/MurUEJL/1998/3.html>.

Thornthwaite discusses the following two cases as examples of decisions that favour employees in their complaints against unfair dismissals when information has been obtained from their personal SMedia sites without their consent or knowledge.[440] These decisions are indicative that the FWC is, as Thornthwaite points out, leaning towards a concept of '*emerging privacy*' (emphasis added) in relation to an employee's SMedia sites as a personal space.[441]

In the case of *Wilkinson-Reed v Launtoy Pty Ltd* [2014] FWC 644, the employee (Wilkinson-Reed) had been an exemplary employee for 18 years when she was summarily dismissed for an alleged breach of confidentiality in discussing workplace matters with her superior's wife. Allegedly, these communications were both in breach of her superior's specific instructions as well as the company's SMedia policy. Wilkinson-Reed communicated with her superior's wife through private messaging on her Facebook page. The communication was held not to be a breach of confidentiality or a breach of the employer's SMedia policy, because her manager retrieved the communication through an improper access of his wife's Facebook page.[442] The employer would not have had knowledge of the communication without the manager's improper and unauthorised access of his wife's Facebook page and messages.[443] The FWC considered the fact that the employee had genuinely believed her conversation was private as it was not made through a Facebook post but through a private message and not intended for the public domain of SMedia.[444]

[440] Thornthwaite, above n 401, 8, 10.
[441] Ibid.
[442] *Wilkinson-Reed v Launtoy Pty Ltd* [2014] FWC 644 [63].
[443] Ibid.
[444] Ibid [66].

In addressing the actual content of the conversation, the FWC held that an employee has a right to discuss their work life.[445] In the absence of something more like an actual breach of confidentiality, mere comments or opinions about an employer or how others view an employer will not be sufficient to uphold a summary dismissal.[446] The fact that this conversation took place on SMedia did not automatically render it a 'public' conversation.[447] In relation to the appropriateness of the company's SMedia policy, Commissioner Deegan also commented on the difficulties with policies that attempt to regulate an employee's private communications regardless of a connection to the employment relationship. He stated:

> it is unlikely that a policy that was an attempt by an employer to control the contents of private emails between their employees' third parties, written in their own time and using their own equipment, would be found to have the requisite connection to the employment relationship such that an employee could be terminated for a breach.[448]

Similarly, in *Fallens v Serco Australia Pty Ltd* [2015] FWC 8394 the employer (Serco) obtained access to the employee's (Fallens') SMedia communication through the employee's separated spouse. The FWC found that the employer's acceptance of such communication that included the employee's Facebook messages that were accessed by the estranged spouse from the employee's computer was inappropriate, bearing in mind the estranged nature of their marriage at the time the communications were provided to the employer.[449] The FWC went on to say 'Impropriety between spouses involving unauthorised access to and distribution of

[445] Ibid [69].
[446] Ibid.
[447] *Wilkinson-Reed v Launtoy Pty Ltd* [2014] FWC 644 [66].
[448] Ibid.
[449] *Fallens v Serco Australia Pty Ltd* [2015] FWC 8394 [20].

private documents should be discouraged. The social consequences of such conduct cannot be positive'.[450] Again, the Court expressed a clear indication that any employer access to employee SMedia should be done in an ethical manner and that the mere fact of a communication being on SMedia does not mean it is in a public forum. It is not for the employer to access SMedia communications in any manner they see fit.

3.2.2. Analysis of case law

It is worth reviewing five of the cases previously discussed: *Linfox Australia Pty Ltd v Fair Work Commission and Stutsel*, *Vosper v Solibrooke Pty Ltd*, *Starr v Department of Human Services*, *Wilkinson-Reed v Launtoy Pty Ltd* and *Fallens v Serco Australia Pty Ltd*. In these cases, the FWC upheld employee allegations that they had been unfairly dismissed due to communications the employees had posted on their personal SMedia sites. Some of the pertinent factors the FWC will consider in determining such matters include: the privacy settings of the SMedia sites,[451] the characteristics of the dismissed employee (eg, level of digital literacy including knowledge of how SMedia sites operate),[452] the employee's length of service,[453] age, position at work, the possibility of the employee obtaining another position[454] and the ethicality of how the employer obtained the employee's communication on

[450] Ibid.
[451] *Wilkinson-Reed v Launtoy Pty Ltd* [2014] FWC 644 [21] [35]; *Vosper v Solibrooke Pty Ltd* [2016] FWC 1168 [37].
[452] *Linfox Australia Pty Ltd v Fair Work Commission and Stutsel* [2013] FCAFC 157.
[453] Ibid [3],[4]; *Vosper v Solibrooke Pty Ltd* [2016] FWC 1168, [37]; *B, C and D v Australian Postal Corporation* [2013] FWCFB 6191 [88]; *Starr v Department of Human Services* [2016] FWC 1460 [5] (upheld on appeal).
[454] *B, C and D v Australian Postal Corporation* [2013] FWCFB 6191 [88]; *Starr v Department of Human Services* [2016] FWC 1460 [5] (upheld on appeal).

SMedia.[455] The FWC also examined whether any harm had been caused to the employer by the communication in dispute.[456] In all the above cases the FWC held that no harm, or at least no harm sufficient to result in the dismissal of the employee, had ensued. A review of decisions in older cases may well reveal a knee jerk reaction to the sudden and, at that time, unknown phenomena of SMedia for which the courts were ill prepared.[457] These cases are reviewed below in the context of employee duties of fidelity and obedience.

Thornthwaite discusses the newer cases in light of an employer's control of an employee's activities outside work hours (ie, during an employee's private time).[458] In this instance, the discussion in this thesis revolves around SMedia as a sphere caught between the dichotomy of public and private communication. This view follows Nissenbaum's argument that even information accessible in a public forum can still be private to the person it relates to or was created by.[459] The newer cases discussed above reveal a cautious familiarity with SMedia as a contemporary and pervasive mode of social communication for all ages and levels that is not a fad, but is here to stay. The reality is that workplace interaction is no longer confined to breaks at the coffee machine. Social human interaction at work or about work often includes real-time communication on SMedia even as work goes on in open cubicles or shared spaces. The loss of audio and visual spatial privacy has led to online

[455] *Fallens v Serco Australia Pty Ltd* [2015] FWC 8394 [17] [20]; *Wilkinson-Reed v Launtoy Pty Ltd* [2014] FWC 644 [21] [35].
[456] *Vosper v Solibrooke Pty Ltd* [2016] FWC 1168 [21].
[457] See *Little v Credit Corporation Group Ltd* [2013] FWC 9642; *Dover-Ray v Real Insurance Pty* (2010) 204 IR 399; *O'Keefe v William Muir's Pty Ltd* [2011] FWA 5311; *Mayberry v Kijani Investments Pty Ltd ATF The Dawe Investments Trust Subway Wallsend* [2011] FWA 3496.
[458] Louise Thornthwaite, 'Social Media and Dismissal: Towards a Reasonable Expectation of Privacy?' *Journal of Industrial Relations* 1–18.
[459] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press, 2010) 231.

'private' messaging on SMedia as an avenue of communication for younger workers and non-senior management who may not have access to individual private offices. Thornthwaite[460] and van Dissel[461] appear to share a common perspective with regards to allegations of unfair dismissal and employee SMedia communication. They consider all such communication as occurring while 'off duty' or resulting from 'conduct outside work' and see restrictions as a form of employer control over employees' freedom of speech 'outside work' hours. Theirs is a legitimate perception.

However, in the cases discussed in Part 3, not all the employee comments that have led to dismissal were made during work hours. For example, in *Starr v Department of Human Services* the comments relating to Starr's dismissal were made during his free time.[462] However, the disputed comments were made about work-related matters and people on SMedia, a space that is commonly regarded as a public forum.[463] It would appear that the initial rush to protect employers from malicious, reckless or careless employee comments on SMedia as a public forum is slowing down. This thesis submits that the courts' growing familiarity with technology and the sheer ubiquity of SMedia as a forum of community social interaction is resulting in the courts moving their focus towards finding a fairer balance between protecting employers from harm and employees' individual privacy. This perspective may provide some explanation of the growing trend towards decisions that seem to accept SMedia as a public forum, but which incorporate aspects of protected private

[460] Thornthwaite, above n 401, 8, 9.
[461] van Dissel, above n 118, 222, 224, 228.
[462] *Starr v Department of Human Services* [2016] FWC 1460 [18].
[463] van Dissel, above n 118, 222, 228.

communications in relation to employees. This view is supported by Thornthwaite's comments regarding the aforementioned cases in which she states FWC judgments recognise that employees may have a right to a reasonable expectation of privacy.[464]

Most other countries have some form of entrenched legislative protections for freedoms of speech and self-expression. For example, the UK has enacted the *Human Rights Act 1989* (UK) that incorporates Article 8 of the *European Convention of Human Rights* into its domestic law. Article 8 provides a right to a reasonable expectation of privacy in an individual's private life. The *Human Rights Act* 1989 (UK) has had the effect of requiring UK industries, tribunals and employment laws to interpret and apply its laws and decisions in such a way as to give employees a 'reasonable right of privacy'.[465] Similarly, the Supreme Court of the United States has conclusively established the concept of 'a reasonable right to privacy'.[466] The Court established a two-step test, in which step one is to determine if a person has shown a real expectation of privacy.[467] An example of this could be through managing their SMedia privacy settings. If the first step of the test is met, then it is necessary to determine if that expectation is a reasonable one to have.[468] In the context of individual employee privacy and SMedia, it would seem that controlling privacy settings, managing the people who can view your posts or have access to share them and using private messaging or private groups with trusted members are

[464] Thornthwaite, above 457, 1, 3.
[465] Thornthwaite, above n 457,1, 4.
[466] *Katz v United States* 39 US 347 (1967).
[467] Ibid 361.
[468] Ibid.

some of the ways that an individual may show a reasonable expectation of privacy.[469]

3.3. Scope and Ambit of Duties Employees Owe Employers to Restrain Freedom of Speech

From an employee's expectations in relation to privacy this discussion now proceeds to the second interrelated issue. The task is to determine the scope, if any, of duties that employees owe to their employer to restrain the employees' 'freedom' of speech when communicating opinions about their work, employer or any other work-related matter through SMedia. Various duties owed by employees to employers were discussed in Part 2. Following that discussion, the two duties now discussed are the employees' duty of fidelity and the duty to obey.

3.3.1. Duty of fidelity

It has been said that the employee's duty of fidelity encompasses 'loyalty, honesty and confidentiality'.[470] The duty can be described as a duty to act in the best interests of the employer and, in particular, the employee should not act in a manner that is detrimental to the employer or the workplace.[471]

---

[469] See, eg, European Union Agency for Law Enforcement, *How to Set Your Privacy Settings on Social Media*, Europol <https://www.europol.europa.eu/how-to-set-your-privacy-settings-social-media>; Nahier Aldhafferi, Charles Watson and A S M Sajeev, 'Personal Information Privacy Settings of Online Social Networks and Their Suitability for Mobile Internet Devices' (2013) 2(2) *International Journal of Security, Privacy and Trust Management* 1, 4.
[470] *Concut Pty Ltd v Worrel* (2000) 176 ALR 693, citing *Blyth Chemicals v Bushnell* (1933) 49 CLR 66, 81–82, stating that the duty of fidelity and good faith is a multi-pronged.
[471] *State of South Australia v McDonald* (2009) 104 SASR 344, cited in Beatrix M P van Dissel, 'Social Media and the Employee's Right to Privacy in Australia' (2014) 4(3) *International Data Privacy Law* 222.

Canadian academic Robert Flannigan describes the duty of fidelity as employees entering into a 'limited access' employment relationship for a self-interested purpose.[472] This is the case when they are using their employer's resources and their own labour or skill.[473] Employees circumscribe the use of their employer's resources for the employer's benefit, as with their own labour or skill.[474] Flannigan goes on to note that, as a result of this limited access relationship 'employees must forgo unauthorised conflicts and benefits'.[475] I interpret this to mean that employees impliedly agree to subordinate their own interests to forward the interests of their employer in return for the employment relationship. It is an iteration of the 'work–wages' bargain.

This raises the question as to what this duty entails from the employee. How much does an employee need to subsume his own freedoms of speech and expression to 'protect' his employer's privacy of workplace conduct, information, confidentiality (ie, secrets and work processes) and reputation from harm?

Case law indicates that the courts framed this duty generously to favour the employee. For example, in *Rose v Telstra Corporation Ltd* [1998] AIRC 1592 the Australian Industrial Relations Commission (AIRC) held that:

> employers do not have an unfettered right to sit in judgment on the out-of-work behaviour of their employees. An employee is entitled to a private life. The

[472] Robert Flannigan, 'Constructing an Employee Duty of Fidelity?' (2016) 37(2) *Business Law Review* 50. Robert Flannigan is a Professor of Law at the University of Saskatchewan and a guest contributor to the Oxford Business Law Blog.
[473] Ibid.
[474] Ibid.
[475] Ibid.

> circumstances in which an employee may be validly terminated because of their conduct outside work are limited.[476]

An employee's behaviour may only result in a breach of this duty when such behaviour results in detriment to the employer and is in breach of a contractual term of employment, either expressly or impliedly (eg, through a workplace policy that is incorporated into the contract of employment).[477] The requirement for a breach of a contractual term is to ensure that employers are able to show the nexus between the employee's improper actions, their dismissal and the employment relationship.[478]

A key component of this duty, as is recognised in the case law, is that the employee's breach must have caused harm, detriment or some form of negative effect to the employer or the workplace (eg, to other employees, customers' perception of the employer and so forth).[479] This is exemplified in the case of *Blyth Chemicals v Bushnell* (1933) 49 CLR 66 — the benchmark for defining 'harm' in relation to this duty. In this case, the court required 'an actual repugnance between the individual acts and the employment relationship and that it was not enough that grounds for uneasiness as to future conduct arises'.[480] In the context of SMedia, this requirement for harm relates to the second tension described by Brown and Dent, that is, the extent to which SMedia posts may effect the employer.[481] The Court in *Rose v Telstra Corporation Ltd* [482] explained that for a summary dismissal for an alleged

[476] *Rose v Telstra Corporation Lt*d [1998] AIRC 1592, xx.
[477] Ibid.
[478] Ibid.
[479] *Blyth Chemicals v Bushnell* (1933) 49 CLR 66, 81–82; *Rose v Telstra Corporation Lt*d [1998] AIRC 1592.
[480] *Blyth Chemicals v Bushnell* (1933) 49 CLR 66, 81–82.
[481] Brown and Dent, above n 329, 4.
[482] *Rose v Telstra Corporation Lt*d [1998] AIRC 1592.

breach of duty of fidelity to be upheld the conduct of the employee had to be of such severity that it amounted to a rejection of the contract of service.[483]

In the absence of any contemporary legislation regulating the privacy of employees on SMedia, the doctrine of precedent has resulted in the courts using the existing principles as best as they can in deciding claims of unfair dismissal resulting from employee's after-work communications on personal SMedia.[484]

3.3.1.1. Duty of fidelity post-SMedia

An early example of a court finding that the duty of fidelity had been breached due to communications on SMedia is found in *O'Keefe v William Muir's Pty Ltd* [2011] FWA 5311. In this case, the employee (O'Keefe) posted several comments on his SMedia that he claimed were made on his home computer outside business hours.[485] O'Keefe also claimed that his posting could not be linked to his employment as there was no mention of the employer by name.[486] O'Keefe admitted that he was aware he had colleagues on SMedia who could see his comments.[487] O'Keefe stated that he did not intend for the comments to be seen by the co-worker he had alluded to in his comments.[488] The court considered it unlikely that O'Keefe was unaware of the consequences of his behaviour.[489] On the facts, O'Keefe was dismissed because his comments constituted sexual harassment and were threatening towards a co-worker. Deputy President Swan upheld the dismissal stating that 'the manner in

[483] Thornthwaite, above n 457, 1, 8.
[484] Thornthwaite, above n 457, 1, 7.
[485] *O'Keefe v Williams Muir's Pty Ltd* [2011] FWA 5311 [43].
[486] Ibid [16].
[487] Ibid.
[488] Ibid [35].
[489] Ibid [39].

which the threat was made and the words used provided sufficient reason for the respondent's dismissal of the applicant on the grounds of serious misconduct'.[490] Deputy President Swan also stated 'the separation between home and work is now less pronounced than it once used to be'.[491] It did not make a difference that O'Keefe made the comments on his home computer or outside business hours.[492]

In *Dover-Ray v Real Insurance Pty Ltd* (2010) FWA 8544, the employee (Dover-Ray) accused her manager of sexual harassment. After an investigation, the employer (Real Insurance), found her allegation to be unsubstantiated. Dover-Ray criticised her employer's conduct of the investigation on her SMedia account, a MySpace page. She referred to her employer as 'nothing but witch hunters'.[493] When Dover-Ray was issued with a show cause order, she lodged an unfair dismissal claim with the FWC. Her employer responded by lodging a Notice of Representation in which they stated that Dover-Ray had not been terminated and she was free to return to work at any time, but only if she removed the MySpace post. On the facts, although the employer was not identified by name, the Court found that it did identify Dover-Ray, was dated and related to her workplace experience.[494] This meant it would have been clear to anyone who knew Dover-Ray that she was referring to her employer.[495] The Court held that the dismissal was valid because Dover-Ray had published the comment on SMedia.[496] The manner of publication allowed her employer to be identified and resulted in reputational harm to the employer. Her

[490] *O'Keefe v Williams Muir's Pty Ltd* [2011] FWA 5311 [51].
[491] Ibid [43].
[492] Ibid.
[493] *Dover-Ray v Real Insurance Pty Ltd* (2010) FWA 8544 [22].
[494] Ibid [53].
[495] Ibid.
[496] Ibid [79].

refusal to modify or remove it was a breach of her implied contractual obligations. Although the court did not categorically mention the duty of fidelity, Commissioner Thatcher did point out the harm caused to the employer:

> The blog is, in effect, an attack on the integrity of the management of Real. The criticism of corruption is of such a nature and degree that it cannot be brushed aside by the submission on behalf of Ms Dover-Ray that Mr Grobler [her manager] was being 'precious' by being personally offended by the criticism within the blog.[497]

Causing such harm to the employer is a clear breach of the employee's duty to act in the best interests of the employer. Additionally, Commissioner Thatcher found that Dover-Ray's explanation regarding the privacy of her SMedia site was contradictory.[498] In this instance, the Court held that Dover-Ray had made disparaging comments on SMedia knowing that it would be communicated outside her SMedia friends and spread to her workplace.[499] Commissioner Thatcher went on to highlight that Dover-Ray's 'friends' on SMedia included other employees in the same organisation.[500] This clearly increased the likelihood of Dover-Ray's comments spreading into her employment space which would foreseeably lead to an undesirable effect on her employer's reputation. In this context, it is similar to *O'Keefe v William Muir's Pty Ltd* as it is unlikely Dover-Ray would have not been aware of the consequences of her comments on SMedia.

The Full Bench of the FWC recently upheld a similar dismissal in *Pearse v Viva Energy Refining Pty Ltd* [2017] FWCFB 4701. In this instance, the employee

[497] Ibid [55].
[498] Ibid [50].
[499] Ibid.
[500] Ibid. [51].

(Pearse) sent an email that contained criticisms and allegations to approximately 170 fellow workers.[501] The criticisms and allegations were directed against the 170 fellow workers.[502] The dismissal was upheld as valid on the grounds that the employee had not 'sought to recall the email, did not seek to reissue it in a less emotive or derogatory form and the email was not remediated when it could have been'.[503] In both *Dover-Ray v Real Insurance Pty Ltd* and *Pearse v Viva Energy Refining Pty Ltd* the employees breached their duty of fidelity by bringing their employers and fellow employees into disrepute. Both employers alleged a breach of workplace policies, even though neither employer had a SMedia policy in place.

In the above cases, the court appears to have interpreted the duty of fidelity strictly. This seems to be in part because the employees refused to remove or moderate the harm caused by removing their posts or apologising for them. They had caused harm to the employer because the posts could be viewed by other employees.

Wilkinson-Reed v Launtoy Pty Ltd discussed above had a different outcome. In that case, an employee's conversation on Facebook messaging regarding a superior being a 'narcissist' occurred outside work hours and was held to be acceptable and not grounds for dismissal.[504] It could be said that Wilkinson-Reed did not breach her duty of fidelity, as her messages were made through private messaging with no intention to circulate outside the confines of her private conversation. In addition, the Court did not find that any harm had occurred to the employer.

[501] *Pearse v Viva Energy Refining Pty Ltd* [2017] FWCFB 4791 [4].
[502] Ibid.
[503] Ibid [17].
[504] *Wilkinson-Reed v Launtoy Pty Ltd* [2014] FWC 644 [69].

In *Fitzgerald v Smith* [2010] FWA 7358, Commissioner Bisset acknowledged the decision in *Rose v Telstra Corporation Ltd*[505] and agreed that behaviour outside working hours may have an effect on employment 'to the extent that it can be said to breach an express term of [an employee's] contract of employment'.[506] With specific reference to SMedia, Commissioner Bisset stated that even if it is made outside working hours, a Facebook post does not stop having effect once work resumes.[507] He went on to categorically state that 'It would be foolish of employees to think they may say as they wish on their Facebook page with total immunity from any consequences'.[508]

In this instance, the employee (Fitzgerald) posted a sarcastic message on her Facebook page indicating her unhappiness with her Christmas bonus and the arrangements for holiday pay on or about end of December 2009 after she received her pay on 23 December 2009.[509] The employer became aware of the comments through a third party, but did not respond until 9 February 2010 when she terminated Fitzgerald's employment. The Commissioner took the employer's slow response as pointing to a lack of the harm that is required before the right to dismiss an employee arises. In addition, Fitzgerald removed the comments from her Facebook page within a few weeks of posting them.[510] Her willingness to mitigate any potential harm was unlike the employees' behaviour in the cases of *O'Keefe v William Muir's Pty Ltd*

[505] *Rose v Telstra Corporation Ltd* [1998] AIRC 1592.
[506] *Fitzgerald v Smith* [2010] FWA 7358 [51].
[507] Ibid [52].
[508] Ibid.
[509] Ibid [19], [21].
[510] Ibid [21].

and *Dover-Ray v Real Insurance Pty Ltd* and is part of the reason her dismissal was unfair.

Although Fitzgerald had restricted the privacy settings and only intended to post to her Facebook friends, the Commissioner took two factors into account. First that her employer found out about the posts through a third party.[511] Second that the employer's clients were among Fitzgerald's Facebook friends.[512] This led Commissioner Bisset to comment that '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'.[513] However, ultimately the Commissioner ruled that Fitzgerald's dismissal was unfair.[514] His decision was upheld by the Full Bench of the Fair Work Commission.[515]

These above cases underscore the fact that, while employees are allowed to make public comments about their employer, for example, on SMedia, employees will be held responsible for the harm that may ensue to the employer from an indiscreet or careless comment. Employees' implied freedoms of speech and expression must be balanced against their duty of fidelity to protect the employer from harm when making comments about an employer on SMedia. One way to attempt this balance is for employees to ensure their SMedia communication is set to the highest privacy settings, as was noted by the court in *Linfox Australia Pty Ltd v Stutsel*.[516]

---

[511] Ibid [49].
[512] Ibid [55].
[513] Ibid [50].
[514] Ibid [66].
[515] *Smith v Fitzgerald* [2011] FWAFB 1422 [16]. The Full Bench of Fair Work Australia quashed the remedy and remitted the case back to Commissioner Bissett for review, see [20]–[21].
[516] *Linfox Australia Pty Ltd v Glen Stutsel* [2012] FWAFB 7097 [33] [19].

3.3.2. Duty to obey

The duty to obey an employer was mentioned in Part 2 and will be discussed now in relation to whether or not employees are required to obey employers' instructions with regard to employees' personal SMedia communications.

Historically, an employee's duty to obey reasonable instructions is a residue of the master–servant relationship in which 'servants' had a duty to 'obey' their masters at all times.[517] An underlining foundation of the master–servant relationship was that an employer had absolute control over all areas of his employee's life.[518] When a servant's disobedience ceased to be a matter for the criminal law, the relationship between employer and employee became one between supposed equals under common law principles of contract.[519] During this evolution of the employment relationship from master–servant to employer–employee, an employee's duty of fidelity (discussed in section 3.3.1) was considered as merely an aspect of the duty to obey.[520] In 1959, Lord Evershed laid down the two limbs of this duty.[521] His Lordship stated that a wilful disobedience of a lawful and reasonable order would justify summary dismissal, as that disobedience showed a complete disregard of an essential condition of the contract of service.[522] This has been incorporated into

[517] Sir Otto Kahn-Freund, 'Blackstone's Neglected Child: The Contract of Employment' (1977) 93 *Law Quarterly Review* 508, 521.
[518] Thornthwaite, above n 16, 164.
[519] *Emmens v Elderton* (1853) 4 HLC 624; 10 ER 606; see Adrian Merritt, 'The Historical Role of Law in the Regulation of Employment' (1982) 1 *Australian Journal of Law and Society* 56; Simon Deakin and Frank Wilkinson, *The Law of the Labour Market: Industrialization, Employment, and Legal Evolution* (Oxford University Press, 2005) 79, 107, cited in n 14 in Andrew Frazer, *The Employee's Contractual Duty of Fidelity* (2015) University of Wollongong Research Online <http://ro.uow.edu.au/lhapapers/2057/>.
[520] Frazer, above n 109.
[521] Ibid 700.
[522] Lord Evershed MR in *Laws v London* [1959] 1 WLR 698 CA 700.

Australian employment law in the Act[523] and Fair Work Regulations that read together define 'serious misconduct' as conduct that includes the 'wilful or deliberate behaviour by an employee that is inconsistent with the continuation of the contract of employment',[524] or when the employee refuses to carry out a lawful and reasonable instruction that is consistent with the employee's contract of employment.[525] Such intentional disobedience amounts to a *serious misconduct* and is a ground for summary dismissal. The current law does not elaborate the concept of serious misconduct and does not provide adequate definition. The Act only refers to the concept of 'serious misconduct' in three sections, as detailed in the following excerpt from *Sharp v BCS Infrastructure*.[526] In that matter, the Full Bench of the Commission said: 'The relevance of the definition of "serious misconduct" in reg.1.07 to the matter is also, with respect, obscure. Section 12 of the Act contains a definition of "serious misconduct" for the purposes of the Act which simply cross-refers to reg.1.07. Apart from s.12 itself, the expression "serious misconduct" is used in only three places in the Act. In s.123(1)(b), a dismissal for serious misconduct is a circumstance in which the notice and redundancy entitlement provisions of Pt 2-2 Div 11 are not applicable; in s.534(1)(b) a dismissal for serious misconduct is one to which the requirements for notification and consultation in Pt 3-6 Div 2 do not apply; and in s.789(1)(b) a dismissal for serious misconduct is one in relation to which the requirements established by Pt 6-4 Div 3 for notification and consultation do not apply. The expression "serious misconduct" is not used anywhere in Pt 3-2, Unfair

[523] Section 12 *Fair Work Act 2009* (Cth) provides that 'serious misconduct' has the meaning prescribed by the regulations.
[524] Reg 1.07(2)(a) Fair Work Regulations 2009 (Cth).
[525] Reg 1.07(3(c)) Fair Work Regulations 2009 (Cth).
[526] *Sharp v BCS Infrastructure Support Pty Ltd* [2015] FWCFB 1033.

Dismissal, of the Act. Section 392(3) requires the Commission, in relation to the award of compensation for an unfair dismissal, to reduce the amount that it would otherwise order by an appropriate amount where it is "satisfied that the misconduct of a person contributed to the employer's decision to dismiss the person". However, it is clear that conduct may constitute "misconduct" for the purpose of s.392(3) without necessarily being "serious misconduct".'[527]

The common law from which this duty derived provides more explanation in relation to the definition and scope of this duty and is discussed below. As stated in Part 2, some of the cases used as examples may not be directly relevant to the specific context of this paper; however, they serve to highlight the salient aspects of this duty. The *lawfulness* of an order is more easily determined than the *reasonableness* of an order. A 'lawful' direction is one in which the employer does not require the employee to contravene a state, territory or Commonwealth law, is in harmony with the employee's contract of service and any applicable award, enterprise agreement or other such instruments.[528] In addition, the order to the employee must be given from a person who has the authority to do so[529] and must be an order that requires actions that are within the qualifications or skill sets of the employee.[530] Generally, the court will consider all the surrounding circumstances of a case to determine if an employer's order to his employee is reasonable.[531] An example of a case in which the court held that an employer's order to follow a conventional dress code at work

[527] *Sharp v BCS Infrastructure Support Pty Ltd* [2015] FWCFB 1033 [33].
[528] van der Waarden, above n 343, 117 [6.5].
[529] *Australian Telecommunications Commission v Hart* [1982] FCA 197.
[530] *Tran v Callum Textiles Pty Ltd* (1997) 42 AILR 3-553 (No VI 1401 of 1996). In this case, a receptionist who was asked to wash teacups was held to have lawfully refused to do so as washing up was not within the scope of her contract of employment as a receptionist.
[531] van der Waarden, above n 343, 116 [6.3].

was both lawful and reasonable is *Australian Telecommunications Commission v Hart* [1982] FCA 185.[532] In this instance, the employee (Hart) refused to follow a dress code stipulated by the employer (Telecom)[533] and so was dismissed. Hart wore a caftan to work.[534] Telecom wanted him to dress more conventionally, as other employees did.[535] Telecom did not have any policy or by-laws in relation to a dress code.[536] However, the orders as to a dress code were given to Hart by a person with authority to do so in accordance with the relevant statute regulating Telecom.[537] The majority of the Full Federal Court held that Hart's disobedience resulted in a direct breach of his contract of service.[538] The orders to comply with a prescribed form of conventional dressing in the workplace were held to be both lawful (as it was given to him by an authorised person as prescribed by the statute) and reasonable (in light of Telecom as a public service employer).[539]

In *Woolworths Ltd v Brown* PR 963023 (26 September 2005), the employer (then known as Safeway) terminated the employee (Brown) for an alleged breach of the Safeway dress policy.[540] The alleged breach was in relation to an eyebrow ring he wore but which he covered by a blue bandaid when he was at work.[541] There was

---

[532] *Australian Telecommunications Commission v Hart* [1982] FCA 185; (1982) 43 ALR 165.
[533] Ibid [20].
[534] Australian Telecommunications Commission v Hart [1982] FCA 185.
[535] Ibid.
[536] Ibid.
[537] Section 57 of the Telecommunications Act 1975 creates an offence of failure of an officer to fulfil his duty as an officer and s 58(1) provides that an officer shall be taken to have failed to fulfil his duty as an officer if and only if 'he wilfully disobeys or wilfully disregards a direction given to him as an officer and given by a person having authority to give the direction' as stated in the headnote to *Australian Telecommunications Commission v Hart* [1982] FCA 197.
[538] *Australian Telecommunications Commission v Hart* [1982] FCA 197.
[539] Ibid.
[540] *Woolworths Ltd v Brown* PR 963023 (26 September 2005). A Full Bench of the AIRC gave the order confirming Senior Deputy President Acton's determination. The pinpoint comes from *Brown v Woolworths Ltd* PR958576 [2005] AIRC 498 [9].
[541] Ibid.

conflicting evidence between the employer and the employee as to whether he had permission to wear the eyebrow ring (covered by the blue bandaid) when he was working.[542] Senior Deputy President Acton accepted the employee's evidence that the employer had granted him permission to wear the eyebrow ring covered by a blue bandaid when he was at work[543] and consequently determined that the employee should not have been dismissed. Among the factors that the court took into consideration were that Brown had worked at Safeway with his eyebrow ring for more than two years without issue and without affecting 'the viability of the undertaking, establishment or service of Safeway'[544] and the eyebrow ring as it was worn did not breach any health or safety laws.[545] In short, and significantly, apart from the issue of being granted permission, the fact that the employer had suffered no harm as a result of the employee's conduct was a factor in the court's decision.[546] On appeal, the Commissioners acknowledged that workplace policies are a necessity for employers seeking to ensure compliance with various duties, both statutory and at common law.[547]

In *Sharp v BCS Infrastructure Support Pty Ltd* [2015] FWCFB 1033 BCS, the employer (Infrastructure Support Pty Ltd) dismissed the employee (Sharp) for breaching the employer's policies of zero tolerance towards the use of drugs or alcohol in the workplace. The employee acknowledged being aware of the policies and having received requisite training in relation to those policies.[548] On appeal

[542] *Brown v Woolworths Ltd* PR958576 [2005] AIRC 498 [15].
[543] Ibid [16], [19].
[544] Ibid [44].
[545] Ibid [45].
[546] Ibid [45].
[547] Ibid [24].
[548] *Sharp v BCS Infrastructure Support Pty Ltd* [2015] FWCFB [14].

against the dismissal, the FWCFB upheld the decision of Vice President Catanzariti that the evidence showed the employee fully understood the gravity of his actions in consuming alcohol and drugs in breach of the employer's zero tolerance policy.[549] Significantly, in this case a mere 'imminent risk' to 'reputation, viability or profitability' was held to be a sufficient breach of policies to warrant a dismissal.[550] This is a broader determination than the previous two cases that obliged a more tangible requirement of harm to be suffered for a dismissal to be upheld.

The above are three examples of pre-SMedia cases. They provide some insight into some of the factors that courts considered when interpreting workplace policies in relation to employee duties to obey such policies within the workplace.

An employer has the power and authority under common law to issue instructions in relation to employee conduct if and when actions of an employee detrimentally affect the performance of work at the workplace.[551] The following statement by Commissioner Bissett is indicative that an employee's actions outside work hours, particularly on personal SMedia, does not remain personal to the employee if it can be shown to detrimentally affect the workplace. Commissioner Bissett notes:

> A Facebook posting, while initially undertaken outside working hours, does not stop once work recommences. It remains on Facebook until removed, for anyone with permission to access the site to see. A Facebook posting comes within the scope of a *Rose v Telstra* consideration but may go further. It would be foolish of employees to think they may say as they wish on their Facebook page with total immunity from any consequences.[552]

[549] Ibid [14], [40].
[550] Ibid [15].
[551] *McManus v Scott-Charlton* (1996) 70 FCR 16, 33 [B].
[552] *Fitzgerald v Smith* [2010] FWA 7358 [52].

This brings us to the next phase of the discussion — the employee's duty to obey and the blurring boundaries of 'within' and 'outside' the workplace.

3.3.2.1. Outside the workplace

Pre-SMedia

The question of whether employees are required to obey norms and rules that the employer sets for conduct *outside the workplace* has been a point of contention from the time the employment relationship began its evolution from master–servant to employer–employee.[553] It is an established rule that employers may terminate an employee for an employee's conduct outside work.[554] Vice President Ross Melbourne laid down the conditions outlined in *Rose v Telstra* as follows:

- the conduct must be such that, viewed objectively, it is likely to cause serious damage to the relationship between the employer and employee, or
- the conduct damages the employer's interests, or
- the conduct is incompatible with the employee's duty as an employee.[555]

In essence, the conduct complained about must be of such gravity or importance as to indicate a rejection or repudiation of the employment contract by the employee.[556]

Rose v Telstra was discussed in section 3.3.1. On its facts and in relation to the duty to obey, the employee in *Rose v Telstra* was found to have acted 'foolishly and in error of judgment', but had not crossed the line into a breach of the duty to obey the

[553] Frazer, above n 109.
[554] *Rose v Telstra Corporation Ltd* [1998] AIRC 1592.
[555] Ibid.
[556] Ibid.

workplace policy resulting in a termination.[557] Briefly, the facts of *Rose v Telstra* were that the employee (Rose) became involved in a physical altercation with a fellow employee outside work hours in a hotel in which the two were staying while working for the employer on an outstation assignment. While Telstra disciplined Rose, it did not take any action against the other employee. In a separate criminal prosecution, the other employee was found guilty of maliciously wounding Rose and was sentenced to four months' imprisonment. The employee subsequently resigned. Telstra terminated Rose, alleging that the altercation was a breach of the employer's 'Code of Conduct' (the Code). The Code stated that:

> We should avoid outside activity likely to affect adversely either our work or someone else's (eg, in terms of occupational health and safety), or which could discredit either ourselves or our Company, or which could conflict with the Company interests.

The court found that 'neither employee was in their Telstra uniform, nor were they "on call" '.[558] Rose's foolishness had not detrimentally affected his work or the employer in any significant or even identifiable manner.[559] Therefore, Vice President Ross Melbourne made his decision to hold that Rose should not have been terminated.[560]

Post-SMedia

In recent years, particularly from 2010, the advent of SMedia led to an initial slew of case decisions that seemed to extend employee obedience to workplace norms to

[557] Ibid.
[558] Ibid.
[559] Ibid.
[560] Ibid.

conduct that took place outside the workplace. This resulted in fears of a re-emergence of the total employer control reminiscent of the master–servant relationship.[561] One way in which employers sought to incorporate an ability to govern conduct outside the workplace into an employee's contractual obligation was to create workplace policies, in particular SMedia policies.[562] Courts appear to have encouraged employers to implement a clearly articulated and fairly enforced SMedia policy, as discussed earlier. The following cases are precursors of those discussed earlier, except for *Pearson v Linfox Australia Pty Ltd*.[563] These cases are discussed in relation to an employee's duty to obey the employer outside work hours and, particularly, in relation to the employee's use of personal SMedia accounts.

In *Pearson v Linfox Australia Pty Ltd*, the employer (Linfox) terminated the employee (Pearson) for disobeying four different workplace policies, including an SMedia policy during his employment between the period of July 2012 and May 2013. Ultimately, Commissioner Gregory determined that, despite being warned about the consequences, the employee had demonstrated a consistently repetitive disregard for workplace policies.[564] Thus, his termination was held to be valid.[565] Specifically, in relation to the SMedia policy, the employee had refused to acknowledge the training he had received on two separate occasions. His rationale for such

[561] Thornthwaite, above n 16, 1.
[562] Leila Chacko, 'Dismissals Based on Breach of Employer Policy — Searching for the Boundaries of "Reasonable" ' (2015) 6 W*orkplace Review* 8. Note, at the time of writing this article, Ms Chacko was a paralegal in the litigation team at WorkCover NSW. The article is an edited version of the speech she delivered as a finalist in the 2014 McCallum Medal annual speaking competition at the Fair Work Commission in Sydney. She is currently employed as a contracting officer at the Department of Defence of Australia.
[563] *Pearson v Linfox Australia Pty Ltd* [2014] FWCFB 1870. FWCFB dismissed Pearson's application to appeal. Therefore, all pinpoints and discussions refer only to the judgment in the first instance *Pearson v Linfox Australia Pty Ltd* [2014] FWC 446.
[564] *Pearson v Linfox Australia Pty Ltd* [2014] FWC 446 [51].
[565] Ibid.

disobedience was his protest against what he perceived as an encroachment into his activities outside work.[566] In his determination, Commissioner Gregory went on to make certain observations specifically in relation to the scope and validity of the SMedia policy. He held that a SMedia policy was an appropriate method to protect 'the reputation and security of a business' by setting out employer expectations in relation to employee behaviour on SMedia when it might affect the business negatively — especially as SMedia communication was, in his opinion, not solely intended for 'private consumption'.[567] Thus, the public nature of an employee's SMedia account was an important consideration for Commissioner Gregory in coming to his decision. This is different from the more recent decisions discussed in sections 3.2.1. and 3.2.2. that appear to accept the existence of a private sphere within the (commonly accepted) public nature of SMedia.

In relation to an employer's control of an employee's activities outside work, Commissioner Gregory accepted that 'there are many situations in which an employer has no right to seek to restrict or regulate an employee's activities away from work'.[568] However, he went on to distinguish situations covered by SMedia policies, as such policies operate to protect the brand and security of businesses in what the Commissioner perceived as a public forum. He felt that SMedia policies were a practical means to manage employee expectations and obligations to ensure an employer's legitimate interests were protected. He observed that: 'Clearly there are some obligations employees accept as part of their employment relationship that have application whether they are at work or involved in activities outside of working

[566] Ibid [45].
[567] Ibid [46].
[568] Ibid [47].

hours'.[569] This seems to indicate that the duty to obey is to be extended outside work hours, particularly in relation to SMedia policies. However, on the facts, Commissioner Gregory did note that the employee's refusal to acknowledge the training he received in relation to the operation of the SMedia policy was 'that the acknowledgement he was asked to sign did not actually commit him to abide by the policy.[570] The employer merely required Pearson to acknowledge that he had read and understood it'.[571] In this context, Commissioner Gregory acknowledged that the employer's requirement was both lawful and reasonable in the circumstances.[572] It can be said that the Commissioner found that the employer's request for the employee's acknowledgement not to be a direct assault on his conduct outside work. He noted that the effect of the terms of the SMedia policy may itself have been open to interpretation if disputed at some later time. Again, this can be said to demonstrate that the nexus between the allowable scope for enforcing an SMedia policy and the employee's duty to obey was, and is still, not fixed. The conservative views of Commissioner Gregory hold a slender thread of flexibility.

The above cases provide examples from private sector employment. An early example of a civil servant's obligations to adhere to departmental SMedia policies is found in *Banerji v Bowles* [2013] FCCA 1052. In that case, the employee (Banerji) worked for the Department of Immigration and Citizenship (DIC) as a 'public affairs

[569] Ibid.
[570] *Pearson v Linfox Australia Pty Ltd* [2014] FWC 446 [45].
[571] Ibid.
[572] Ibid [48].

officer'.[573] Banerji acknowledged that she had used her Twitter account to tweet regular comments in relation to:

> (sometimes mocking, sometimes critical) on, for example, (a) the practices and policies of the company that provides security services at Commonwealth immigration detention centres, (b) the immigration policies of the Australian Government, (c) information and comment by the Opposition spokesman on immigration (Mr Morrison), (d) the Minister for Foreign Affairs (Senator Carr), (e) the [then] Prime Minister, (f) the Leader of the Opposition and (g) employees of the Department.[574]

The DIC claimed that Banerji's comments were a breach of the APS Code of Conduct that sets out behavioural guidelines for public servants.

In particular, the DIC relied on s 13(11) of the Public Service Act (PS Act) that states that an 'APS employee must at all times behave in a way that upholds the good reputation of Australia'.[575] However, Banerji claimed that her comments were 'protected' by the 'constitutional right/freedom of political communication' as 'it is evident that they are a simple expression of political opinion, made in her own time away from work'.[576] In her application, Banerji alleged that her employment was about to be terminated for her activities on SMedia, namely her Twitter account.[577] She sought an interlocutory injunction to restrain her employer from terminating her.[578] Judge Neville held that there was no 'unfettered or unbridled' right such as that being claimed by Banerji.[579] In coming to this decision, Judge Neville followed

[573] *Banerji v Bowles* [2013] FCCA 1052, 5 [16].
[574] Ibid 5 [18].
[575] Ibid 15 [63].
[576] Ibid 12 [52].
[577] Ibid 5 [18].
[578] Ibid.
[579] Ibid 23 [102].

the letter and spirit of the law in relation to protecting the freedom of political communication as stated in *ABC v Lenah Game Meats* (2001) 208 CLR 199.[580] He confirmed that any implied protection of such a freedom was not as of right but only to be granted or exercised to protect 'the intended operation of the system of government created by the *Constitution*'.[581] Banerji's application was dismissed.[582] On the facts, the judgment imposed an obligation upon Banerji to obey her contract of employment, Departmental Codes of Conduct (and SMedia policies) seemingly at the expense of her freedom to communicate outside work hours.[583] One other factor that the court considered was that Banerji had made most of her disputed comments while being employed in a second job without the permission from the DIC — in itself a contravention of the APS and her contract of employment.[584]

A broad view of the decision in *Banerji v Bowles* shows that personal freedoms of conduct and communication outside work are clearly subject to the terms of an individual's contract of employment and any SMedia policies or workplace policies that are contained therein. A slightly narrower construct may limit the application of this judgment to civil servants, as their obedience to their 'master' overrides their freedom of political communication because of their position as civil servants. Their employment may forbid them from detracting from the running of the civil service and good governance as determined by the duly elected constitutional government of the day.

---

[580] Ibid 23 [101].
[581] Ibid 23 [101], 24 [105], citing *ABC v Lenah Game Meats* (2001) 208 CLR [198] [199].
[582] Ibid 23 [104].
[583] Ibid.
[583] Ibid.
[584] Ibid.

In contrast, the recent case of *Starr v Department of Human Services*, as discussed in detail in section 3.2.1, is an example of the changing perspective of the judiciary in relation to SMedia activities outside work.[585] However, a major distinguishing point between the two cases is that Starr's application was for relief from an unfair dismissal, whereas Banerji's application was for a pre-emptive interlocutory injunction against dismissal (the fairness or unfairness of which could have been determined at a later date). It is arguable that, in the absence of other factors such as Banerji's breach of other aspects of the APS (ie, taking on a second job), the court may have granted her application as it was only an interlocutory application and not an application for a final determination or prevention against any other disciplinary measures or outcomes.

The following case is an example of how, despite there being no direct post or commentary made by the employee, the simple act of 'friending' students on her personal SMedia account resulted in the employee being censured and punished for breach of the employer's SMedia policy and related workplace policies. In *Applicant v ACT Department of Education and Training* [2012] FWA, the employee (a teacher at a school in Canberra) appealed a finding of misconduct for allegedly breaching the Department of Education and Training Human Resources Directorate Advice No. 02/2009 'Advice on Using Social Networking Websites' and the Teachers' Code of Professional Practice.[586] She was said to have breached the policies 'by having students of W School on her Facebook account friends list and contacting them through her Facebook account'.[587] Her defence that her account had been 'hacked

[585] *Starr v Department of Human Services* [2016] FWC 1460.
[586] *Applicant v ACT Department of Education and Training* [2012] FWA 2562 [1].
[587] Ibid [1].

into' and that she was not personally befriending her students, but only accepted their requests for friendship was rejected by the FWC and the punishment of a one-month reduction in her salary upheld.[588]

A review of the cases in relation to the duty to obey show that the traditional tests, namely those of the 'lawfulness and reasonableness' of the contractual term or SMedia policy is still good law.[589] Significantly, rather than demanding blind obedience, the employer must show that any perceived disobedience or breach of duty to obey has caused real harm to the employer before it can take any action against an employee.[590] In relation to employee activity on personal SMedia, the courts seem to be limitedly supportive of enforcing terms of employment that include SMedia policies, as long as the policies have been incorporated into a contract of employment and the SMedia policy has been brought to the notice of the employee and is enforced fairly and consistently within the workforce.[591] The validity of an employer's action in dismissing an employee for a breach of an SMedia policy is still an open-ended question and much depends on the factual circumstances of each case.[592] However, recently the courts appear to be adopting the view that while obedience to a valid policy is required, dismissal, especially without any warning or correct processes being followed, as a result of any breach may be held to be unfair.[593]

[588] Ibid [30] [89]–[90].
[589] *Rose v Telstra Corporation Ltd* [1998] AIRC 1592.
[590] *Woolworths Ltd v Brown* PR 963023.
[591] *Pearson v Linfox Australia Pty Ltd* [2014] FWC 446 [51].
[592] *Banerji v Bowles* [2013] FCCA 1052.
[593] *Starr v Department of Human Services* [2016] FWC 1460.

The next area to be examined are the rights (if any) that employers have to restrain or monitor employee activity on employees' personal SMedia accounts.

3.4. Employers Rights to Restrain or Monitor

Following from the above, the final point to determine is whether employers have any rights to restrain or monitor their employees' personal SMedia communication.

3.4.1. Scope and ambit of an employer's right to restrain or monitor employees' activity on personal SMedia accounts

3.4.1.1. Employers' right to restrain

This discussion may overlap with cases or principles discussed previously, particularly section 3.3.2. Therefore, the focus is more in the form of a statement than a discussion.

In the workplace

So long as the restraint is clearly enunciated in the contract of employment or workplace policies and is definitively connected to employment-related contact or activities, an employer may restrain an employee from certain activities that harm, or have a real possibility to cause harm, to the employer.[594] In addition to the possible harms such as breach of confidential information and reputational harm in the cases

[594] Thornthwaite, above n 105, 19.

discussed in section 3.3.2, such harm may also include a loss of productivity due to excessive use of SMedia.[595]

Outside the workplace

It has been long established that employers have a limited right to restrain employee conduct outside the workplace.[596] However, the limitation on this right to exercise control outside the workplace has been the subject of many decisions. For example, Justice Finn's comment in *McManus v Scott-Charlton* (1996) 70 FCR 16 provided a clear warning that any restraints on an employee's out-of-work activities should not be extended as of right. He said: 'I am mindful of the caution that should be exercised when any extension is made to the supervision allowed an employer over the private activities of an employee. It needs to be carefully contained and fully justified'.[597] This was reiterated in *Appellant v Respondent* (1999) 89 IR 407, in which the Full Bench of the AIRC said that 'It is only in exceptional circumstances that the employer has a right to extend any supervision over the private activities of the employees'.[598] These statements propose the existence of a necessarily significant connection with an effect upon an employee's work to allow an employer to direct any out-of-hours activity.[599] In addition, to be a lawful direction such restrictions should only be in respect of an employee's conduct that is clearly within the scope of the employment.[600]

---

[595] *Pearson v Linfox Australia Pty Ltd* [2014] FWC 446 [46]. 'An employer is also entitled to have a policy in place making clear excessive use of social media at work may have consequences for employees'.
[596] *Blyth Chemicals v Bushnell* (1933) 49 CLR 66, 81– 82.
[597] *McManus v Scott-Charlton* (1996) 70 FCR 16, 29 [C].
[598] *Appellant v Respondent* (1999) 89 IR 407 [416].
[599] *Blyth Chemicals v Bushnell* (1933) 49 CLR 66, 81– 82.
[600] Ibid [74].

The FWC re-examined the law in relation to determining whether dismissal was an appropriate remedy for an employee who moved beyond the lines of restraint set by the employer in the recent case of *Clarkin v Bechtel Construction (Australia) Pty Ltd* [2017] FWC 1871. Although it does not involve employee conduct on SMedia, this case is particularly relevant as it deals almost exclusively with the applicant's conduct outside work.[601] As established earlier, the general principles of law remain similar even when the conduct involves SMedia activity. In *Clarkin v Bechtel*, Commissioner Williams reiterated:

> *Rose v Telstra Corporation Ltd* (Rose v Telstra) is long established authority on this point. It is clear that in certain circumstances an employee's employment may be validly terminated because of out-of-hours conduct. But such circumstances are limited: the conduct must be such that, viewed objectively, it is likely to cause serious damage to the relationship between the employer and the employee or the conduct damages the employer's interests or the conduct is incompatible with the employee's duty as an employee.[602]

On the facts, the employee (Clarkin) was involved in a domestic dispute with his partner (also an employee of the same employer) at a hotel.[603] They had checked into the hotel to attend a mutual colleague's birthday together with other colleagues and workmates.[604] The dispute took place inside their private room, but was noisy enough to disturb the occupants of the neighbouring rooms.[605] In addition, the employee physically damaged the shower curtain and objects in the room. These damages were paid for by the employee when he checked out of the hotel.[606] The

[601] *Clarkin v Bechtel Construction (Australia) Pty Ltd* [2017] FWC 1871 [215].
[602] *Rose v Telstra Corporation Ltd* (1998) 45 AIR 3, cited in *Clarkin v Bechtel Construction (Australia) Pty Ltd* [2017] FWC 1871 [130].
[603] Ibid [38], [52].
[604] Ibid [48].
[605] Ibid [86].
[606] Ibid [87].

employee had, as part of his contract of employment, acknowledged and accepted the employer's various workplace policies that included a code of conduct known as the Community Code.[607] Among others, the Community Code prohibited drunken behaviour that caused a nuisance in public (as misconduct)[608] and causing wilful damage to community property (as serious misconduct).[609] The reason for the establishment of the Community Code was the employer's sensitivity to maintaining its reputation within the community in the town of Onslow.[610]

Commissioner Williams found that the employee was guilty of misconduct, not serious misconduct.[611] In addition, the misconduct was not a repetitive or continuing act as it had only occurred once.[612] The treatment meted out to the employee was not consistent or fair as the other employee involved had been punished less severely.[613] Commissioner Williams found that dismissal in this case was inappropriate.

This recent case underscores that courts continue to uphold the tenets set down in earlier cases. Employer intrusion into out-of-work activities will only be acceptable in very limited circumstances. To draw an analogy between public and private, a hotel is a public space. However, a dispute between two employees in a personal relationship within the hotel premises (in a private room) that caused a disturbance to other guests (public) was still adjudged to be a private matter that did not amount

[607] Ibid [20], [37].
[608] Ibid [28].
[609] Ibid [30].
[610] Ibid [22]–[25], [162].
[611] Ibid [206].
[612] Ibid [206].
[613] Ibid [209].

to negatively affecting the employer's reputation sufficiently to justify termination. By analogy, while SMedia as such is a public space, an employer has no right to restrain an employee from posting or commenting on their personal SMedia account. Such employee SMedia activity should not be deemed a reason for dismissal without clear harm to the employer or some other cogent reason (eg, the comments being repetitive and or wilful disobedience to an employer's SMedia policy). For example, in *Pedley v IPMS Pty Ltd* [2013] FWC 4282 an employee's dismissal resulting from the use of his LinkedIn account to solicit his employer's clients for his own business was upheld as causing harm to his employer.[614]

3.4.2. Monitoring of employees

Svantesson[615] identifies the different types of privacy violations that may result from employer intrusions into employees' privacy in the workplace. These include drug testing (discussed above), geographical monitoring (such as the use of GPS, presumably through employer-supplied vehicles or mobile phones), telephone monitoring, performance monitoring and email and internet monitoring.[616] He states that as technology has revolutionised employment, employee expectations of privacy in the workplace have undergone an equally express shift. His notes that 'while most people would not expect an employer to open a letter addressed to an employee, email monitoring in the workplace raises few eyebrows'.[617]

[614] *Pedley v IPMS Pty Ltd [*2013] FWC 4282
[615] Professor Dan Jerker B Svantesson, Law Faculty, Co-Director, Centre for Commercial Law, Bond University, Gold Coast, Australia.
[616] Svantesson, above n 202.
[617] Ibid 180.

As discussed in Part 1, there is no specific legislative barrier to preventing employers from monitoring employees. The primary protection is afforded by the *Act* and the *APPs*. Under the *Act*, any information retrieved from an employee's publicly available SMedia accounts would be deemed to be an employer 'collecting' personal information about the employee.[618] However, the *Act* requires that any such information be collected through 'fair'[619] means and, when reasonably practicable, directly from the employee.[620] The information thus collected must also be 'necessary' for the due functioning of the employer's business.[621]

Recent cases such as *Fallens v Serco*[622] and *Wilkinson-Reed v Launtoy*[623] discussed in section 3.2.1 indicate that the courts place a certain importance on how information is obtained. When obtained through unscrupulous means such information may not be sufficient to discipline, let alone dismiss, an employee.[624] Therefore, despite the lack of legislative protection against employer monitoring of employees in Australia the courts may well disallow information that is obtained through unsanctioned monitoring to be used against an employee. However, in *Jurecek v Director of Transport Safety Victoria* [2016] VSC 285 the Victorian Supreme Court held that the employer's conduct in obtaining access and information directly from the employee's SMedia account (Facebook) to be proper.[625] Their

[618] Brown and Dent, above n 329, 13.
[619] APP 3.5.
[620] APP 3.6.
[621] APP 3.1.
[622] *Fallens v Serco Australia Pty Ltd* [2015] FWC 8394.
[623] *Wilkinson-Reed v Launtoy Pty Ltd* [2014] FWC 644.
[624] Ibid [69].
[625] *Jurecek v Director of Transport Safety Victoria* [2016] VSC 285 [154], [166] Note, this case involved the Victorian equivalent of the *Privacy Act 1988* (Cth) and *APPs*, namely the *Information Privacy Act* 2000 (Vic) and *Information Privacy Principles*. This thesis refers to the Commonwealth legislation for consistency.

rationale was that it would have been impractical to request the said employee for information that might have prejudiced her employment.[626] The court held that asking the employee directly may have 'undermined the integrity of the disciplinary process'.[627] As it transpired, the information that was collected from the employee's SMedia account was held to be 'necessary' within the meaning of APP 3.1, as it was information required to carry out the disciplinary investigation.[628]

This brings us to the significant question: what do courts accept as sanctioned monitoring of an employee's personal SMedia site?

Unofficial monitoring, for example, information that is publicly available on an employee's SMedia site and that is accessed (not directly by the employer as happened in *Jurecek*[629] above) by another employee,[630] a client of the employer,[631] or even anonymously[632] appears to be fair game, as courts seem to accept that information openly available does not constitute 'monitoring'.[633] In fact, one of the first cases involving a successful dismissal as a result of evidence from an employee's SMedia account is *Dekort v Johns River Tavern Pty Ltd* [2010] 3389. In that case, an employee who had said he was unfit for work and claimed payment for sick leave was dismissed after his employer found the employee had posted

[626] Ibid [154].
[627] Ibid.
[628] Ibid [166].
[629] *Jurecek v Director of Transport Safety Victoria* [2016] VSC 285.
[630] *Linfox Australia Pty Ltd v Fair Work Commission and Stutsel* [2013] FCAFC 157. In this case, a manager who was not a friend of employee accessed the employee's Facebook and conveyed the information to the employer resulting in employee's dismissal.
[631] *Pedley v IPMS Pty Ltd* [2013] FWC 4282. A client of the employer who was connected to the employee's LinkedIn account brought the employee's conduct of soliciting clients for his own business to the employer's attention. The employee's dismissal was upheld.
[632] *Smith v Fitzgerald* [2011] FWAFB 1422.
[633] Ibid.

photographs of himself at a party.[634] On the facts, there was no indication as to how the employer obtained the said photograph. On the facts, the employee's lack of response or inability to refute the evidence was held to be a core reason for his dismissal being upheld.[635] In *Smith v Fitzgerald* (detailed in section 3.3.1.1), the court clearly accepted that an employer who received information from an employee's personal SMedia account through a third person was able to use the information against the employee.[636] On the facts, the employer's delay in addressing the employee in relation to the information indicated that the employer did not envisage any harm from the post and the dismissal was held to be unfair.[637]

However, the employer's position becomes unclear when the employer obtains information through accessing an employee's communication on employer-held devices. This was briefly discussed in Part 1, using American and European cases as there is no Australian case on point.

4.0 Conclusion

This thesis raises the question of whether there is a judicial trend in relation to unfair dismissals resulting from employee use of personal SMedia accounts.

This thesis explored judicial trends in relation to claims of unfair dismissal lodged by employees dismissed for their posts on SMedia. It found that the law is both underdeveloped and under examined. The sudden influence and rapid growth of SMedia has left legislators behind and courts having to stretch old law to fit new

[634] *Dekort v Johns River Tavern Pty Ltd* [2010] FWA 3389 [4]–[6].
[635] Ibid [16].
[636] *Smith v Fitzgerald* [2011] FWAFB 1422 [9]–[10].
[637] Ibid [16].

circumstance. The historic public–private dichotomy is being recast and it is not clear where the final lines will be drawn.

4.1 Overview of Case Trends Within Australia

This is a review of the cases since 2010, the starting point for employees being dismissed for grounds arising from their activities on their personal SMedia sites.[638] Cases such as *Dekort v Johns River Tavern* did not address the issues of employee activity on personal SMedia accounts in relation to being at work, out of work or whether SMedia was a public or private forum.[639] Although the issue in that case involved a photograph of an employee on his personal SMedia account, the law turned on the employee's failure to 'put any case to meet the assertion of misleading conduct, to explain the inconsistency of his actions or to refute the evidence of the respondent' and his dismissal was held to be fair.[640] Thornthwaite has stated that the evolving nature of the common law-based employee duties of fidelity and obedience, negotiated contractual obligations and current legislative protections (or not) as embedded in the employment legislation provided a probable, more than just possible, potential for 'employees' obligations to be expanded without a reciprocal growth in employers' responsibilities'.[641] This conclusion led to fears that employees may never be able to express honest but detrimental views about their workplaces on their personal SMedia accounts, as they would never be off duty.[642]

[638] Thornthwaite, above n 16, 164,164 [2].
[639] *Dekort v Johns River Tavern Pty Ltd* [2010] FWA 3389.
[640] Ibid 3389 [16].
[641] Thornthwaite, above n 16, 164, 164 [2].
[642] Ibid.

This view seemed to be reinforced in the cases following *Dekort v Johns River Tavern.*[643] For example, in *O'Keefe v William Muir's* [644] Deputy President Swan observed that 'the separation between home and work is now less pronounced than it once used to be'.[645]

However, over the last few years there has been an indication that the courts are willing to find that SMedia is a space that can be construed to be public or private, depending on the privacy settings of the individual. This is apparent from the judgment in *Vosper*[646] and *Starr*.[647] Thornthwaite also suggests that a reading of *Wilkinson-Reed*[648] indicates that when an SMedia site is password protected, the FWC will deem it a sphere of discussion private to the employee.[649] In addition, Thornthwaite is of the opinion that the FWC is likely to hold that it is inappropriate to dismiss an employee due to information that is accessed by the employer through unethical means and without the consent of the employee.[650] This is supported by the analysis of the cases in section 3.4.2. Together with the thrust of the decisions in the other cases discussed in section 3.2.2, this thesis argues that there is a tentative but clear departure from the earlier cases that indicated that 'a discussion on SMedia cannot be regarded in the same light as a discussion in a pub or behind

[643] *Dekort v Johns River Tavern Pty Ltd* [2010] FWA 3389
[644] *O'Keefe v Williams Muir's Pty Ltd* [2011] FWA 5311 [43].
[645] Ibid [51].
[646] *Solibrooke Pty Ltd v Vosper* [2016] FWCFB 2421; *Vosper v Solibrooke Pty Ltd* [2016] FWC 1168.
[647] *Starr v Department of Human Services* [2016] FWC 1460.
[648] *Wilkinson-Reed v Launtoy Pty Ltd* [2014] FWC 644.
[649] Thornthwaite, above n 401,13.
[650] Ibid.

closed doors'.[651] This change in perspective can be traced to *Stutsel v Linfox,* in which Commissioner Roberts observed that within the employee's SMedia activity:

> The chains of comments have very much the flavour of a group of friends letting off steam and trying to outdo one another in being outrageous. Indeed it has much of the favour of a conversation in a pub or cafe, although conducted in an electronic format.[652]

In the same case, on appeal, the FWAFB offered a slightly different characterisation of the employee's SMedia activity as being wider than a 'pub conversation' due to the nature of SMedia as a forum of communication that leaves a permanent and lasting printed commentary that could reach a much wider audience than originally intended by the employee.[653] However, it did go on to say that to sustain a dismissal of an employee, employers need to consider further factors such as the language used, the nature of comments and the intended audience reachability of the publication.[654] The FWAFB stated that 'In this regard we are mindful of the need not to impose unrealistic standards of behaviour and discourse about such matters or to ignore the realities of workplaces'.[655] These comments clearly demonstrate that an employee should not be dismissed merely because of a comment or opinion posted on personal SMedia.

Whether an employee who makes comments on SMedia should be dismissed is more likely to depend on whether such comments cause or are reasonably likely to

[651] *O'Keefe v William Muir's Pty Ltd* [2011] FWA 5311.
[652] *Stutsel v Linfox Australia Pty Ltd* [2011] FWA 8444 [81].
[653] *Linfox Australia Pty Ltd v Stutsel* [2012] FWAFB 7097 [25]–[26].
[654] Ibid [25]–[26].
[655] Ibid [25].

cause actual harm or detriment to an employer. This is in line with the employee's duty of fidelity discussed in section 3.3.1.

As Eric Schmidt, former CEO of Google recently said: 'The internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had'.[656] Anarchy is defined as chaos or lawlessness.[657] In balancing the context of employee personal SMedia activity against employer control (as required to protect business reputation and business entities), the courts are so far unable to depend on the legislature and have to further develop old common law principles. This they do within the constraints of *stare decisis* to provide consistency which is the oppositional pair for flexibility.[658]

In discussing the information age and how law should or could cope with technological advancements, Nigel Wilson[659] notes how the courts, experts and the legal profession all have a part to play in effecting a structure to ensure a current and operational regulation of the information age.[660] He quotes Lord Patten (the former European Commissioner for External Relations): 'Successful legal systems are not static. They develop constantly. And they need to, if they are to keep pace with rapid social and economic change'.[661] I feel that this is the position of the courts

---

[656] Eric Schmidt, as quoted by Saxon R Shaw, 'There is No Silver Bullet: Solutions to Internet Jurisdiction' (2017) *International Journal of Law and Information Technology* 1.
[657] Merriam-Webster Dictionary 'Anarchy' <https://www.merriam-webster.com/dictionary/anarchy>
[658] Roger Brownsword, 'What the World Needs Now: Techno-Regulation, Human Rights and Human Dignity' in Roger Brownsword (ed) *Human Rights* (Hart, 2004) vol 4, 224.
[659] Nigel Wilson is an Adjunct Senior Lecturer at the University of Adelaide Law School. This article is a revised and updated version of his paper delivered at the Australasian Institute of Judicial Administration's Law and Technology Conference, Sydney, 27 June 2008.
[660] Nigel Wilson 'Regulating the Information Age — How Will We Cope With Technological Change?' (2010) 33(2) *Australian Bar Review* 119.
[661] Rising Stars over Europe – Selected Dissertations from EU-China Legal and Judicial Co-Operation Programme, Law Press 2003, [Foreword by Lord Patten], cited by Wilson, above n 659, 127 [8.2].

in Australia, while they wait for legislation to keep up in relation to employer–employee regulation of (unfair) dismissals due to employee use of SMedia. Whatever the response, 'the law cannot be silent'.[662] In this environment of rapid changes in norms of formal and informal privacy it is heartening to see the tentative thread towards a more balanced outlook from the courts in relation to dismissals that come about as a result of activity on an employee's personal SMedia accounts.

[662] Noel Cox, 'Constitutional Responses to Paradigmatic Shifts in Technology' (6 June 2008) *SSRN Electronic Journal* doi:10.2139/ssrn.1140464 <https://www.researchgate.net/publication/228233694_Constitutional_Responses_to_Paradigmatic_Shifts_in_Technology>.Also cited by Wilson, above n 659, 127. Noel Cox is a priest, barrister and researcher specialising in constitutional law and ecclesiastical law and is affiliated with Aberystwyth University, Department of Law and Criminology.

Bibliography

A. Articles/Books/Reports/Conference Papers

Abrahams, Nick and Jamie Griffin, 'Privacy Law: The End of a Long Road: Mandatory Data Breach Notification Becomes Law' (2017) 32 *LSJ: Law Society of NSW Journal* 76

Abril, Patricia Sanchez, Avner Levine and Alissa Del Reigo, 'Blurred Boundaries: Social Media Privacy and the Twenty First Century Employee' (2012) 49(1) *American Business Law Journal* 71

Aldhafferi, Nahier, Charles Watson and A S M Sajeev, 'Personal Information Privacy Settings of Online Social Networks and Their Suitability for Mobile Internet Devices' (2013) 2(2) *International Journal of Security, Privacy and Trust Management* 1.

Andrew, Rachel, Marika Tiggemann and Levina Clark, 'Predicting Body Appreciation in Young Women: An Integrated Model of Positive Body Image' (2016) 18 *Body Image* 34

Asterhan, Christa et al, 'Secondary School Teacher-Student Communication in Facebook: Potentials and Pitfalls' (Paper presented at Chair Conference on Instructional Technologies Research 2013: Learning in the Technological Era, Raanana, 19–20 February 2013)

Asterhan, Christa S C and Hananel Rosenberg, 'The Promise, Reality and Dilemmas of Secondary School Teacher-Student Interactions in Facebook: The Teacher Perspective' (2015) 85 *Computers and Education* 134

Australasian Centre for Policing Research, *Australasian Identity Crime Policing Strategy 2006–2008 of the Australasian and South West Pacific Region Police Commissioners' Conference* (2005)

Australasian Centre for Policing Research and Australian Transaction Reports and Analysis Centre Proof of Identity Steering Committee, *Standardisation of Definitions of Identity Crime Terms: A Step Towards Consistency* (2006)

Australian Law Reform Commission, *Essentially Yours: The Protection of Human Genetic Information in Australia*, Report No 96 (2003)

Australian Law Reform Commission, *Australian Privacy Law and Practice*, Report No 108 (2008)

Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report No 123 (2014)

Bannister, Judith, 'The Public/Private Divide: Personal Information in the Public Domain' (2002) 8(8) *Privacy Law and Privacy Reporter* 157

Barnes, Khaliah and Paige Kowalski, 'Role for Federal Government in Safeguarding Student Data Privacy' (2016) 16(2) *State Education Standard* 18

Bier, William Christian, *Privacy, A Vanishing Value?* (Fordham University Press, 1980), citing Samuel Warran and Louis Brandeis 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193

Brown, Murray, 'Applying for a Job with Big Brother: Is Online Vetting of Job Applicants Lawful in Australia?' (2012) 37(3) *Alternative Law Journal* 186

Brown, Murray and Chris Dent, '*Employer Access to Employee Social Media — Privacy and Regulations'* (2017) 43(3) Monash Law Review (forthcoming)

Brownsword, Roger, 'What the World Needs Now: Techno-Regulation, Human Rights and Human Dignity' in Roger Brownsword (ed), *Human Rights* (Hart, 2004) vol 4

Buchbach, Jacinta, 'Regulating the Boundary Between Work and Self: Emerging Legal Tensions Around Social Media in the Workplace' (Paper presented at the 15th Annual Meeting of the Association of Internet Researchers, Daegu, Korea, 22–24 October 2014)

Butler, Des, 'Protecting Personal Privacy in Australia: Quo Vadis?' (2016) 42(1) *Australian Bar Review* 116

Carney, Andrew, 'Unfair Dismissal Relating to the Use of Social Media — An Analysis of Case History' (2014) 12(1) *Canberra Law Review* 144

Chacko, Leila, 'Dismissals Based on Breach of Employer Policy — Searching for the Boundaries of "Reasonable" '(2015) 6 W*orkplace Review* 8

Cilliers, Francois Quintin, 'The Role and Effect Of Social Media In The Workplace' (2013) 40(3) *Northern Kentucky Law Review* 568

Curlewis, Ian, *Commission Confirms That There is No Contractual Right to Dismiss 'At Will' in Australia* (9 November 2017) Lavan <https://www.lavan.com.au/advice/employment_safety/commission-confirms-that-there-is-no-contractual-right-to-dismiss-at-will-i>

Daly, Angela, ‘The Law and Ethics of “Self-Quantified” Health Information: An Australian Perspective’ (2015) 5(2) *International Data Privacy Law* 144

Deakin, Simon and Frank Wilkinson, *The Law of the Labour Market: Industrialization, Employment, and Legal Evolution* (Oxford University Press, 2005) 79, 107

De Rooy, Julie, ‘Workplace Privacy in a Technological Environment’ (Paper presented at 6th Computer World Conference, Edinburgh, Scotland, 4–8 September 2006) <http://www.law.ed.ac.uk/ahrc/complaw/papers.asp>

Enker, Arnold N, ‘Error Juris in Jewish Criminal Law’ (1994–1995) 11 *Journal of Law and Religion* 23

Espelage, Dorothy L and Jun Sung Hong, ‘Cyberbullying Prevention and Intervention Efforts: Current Knowledge and Future Directions’ (2016) 62(6) *Canadian Journal of Psychiatry* 374

Flannigan, Robert, ‘The Boundaries of Fiduciary Accountability’ (2004) 83 *Canadian Bar Review* 35

Flannigan, Robert, ‘Access or Expectation: The Test For Fiduciary Accountability’ (2010) 89 *Canadian Bar Review* 1

Flannigan, Robert, 'Constructing an Employee Duty of Fidelity?' (2016) 37(2) *Business Law Review* 50

Floyd, Louise and Max Spry, ‘Four Burgeoning IR Issues for 2013 and Beyond: Adverse Action; Social Media & Workplace Policy; Trade Union Regulation (After the HSU Affair) and the QANTAS Aftermath’ (2013) 37 *Australian Bar Review* 153

Forsyth, Anthony, ‘A Thin Wall of Privacy Protection, with Gaps and Cracks: Regulation of Employees’ Personal Information and Workplace Privacy in Australia’ in Roger Blanpain (ed), ’Protection of Employees’ Personal Information and Privacy’ (2014) 88 *Bulletin of Comparative Labour Relations* 7

Fradella, Henry F et al, ‘Quantifying Katz: Empirically Measuring “Reasonableness Expectations of Privacy” in the Fourth Amendment Context’ (2011) 38(3) *American Journal of Criminal Law* 289

Frazer, Andrew, *The Employee's Contractual Duty of Fidelity* (2015) University of Wollongong Research Online <http://ro.uow.edu.au/lhapapers/2057/>

Freedland, Mark, *The Personal Employment Contract* (Oxford University Press, 2003)

Froomkin, A Michael, ‘The Death of Privacy?’ (2000) 52(5) *Stanford Law Review* 1461

Hagedorn, Falk, *Privacy in the Workplace: National Report on Germany* (June 2011) <http://pawproject.eu/en/sites/default/files/page/web_national_report_germany_en.pdf>

Hasday, Jill Elaine, ‘Contest and Consent: A Legal History of Marital Rape’ (2000) 88(5) *California Law Review* 1373

Hernández, Wilnelia, Yair Levy and Michelle M Ramim, ‘An Empirical Assessment of Employee Cyberslacking in the Public Sector: The Social Engineering Threat’ (2016) *CEC Faculty Articles* 340 <http://nsuworks.nova.edu/gscis_facarticles/340>

Hershkovitz, Arnon and Alona Forkosh-Baruch, ‘Student-Teacher Relationship in the Facebook Era: The Student Perspective’ (2013) 23(1) *International Journal Continuing Engineering Education and Life-Long Learning* 35

Holland, Peter, ‘Drug Testing in the Australian Workplace: Still a Contested Terrain’ (2016) 58(5) *Journal of Industrial Relations* 688

Holtfretera, Kirsty et al, ‘Risky Remote Purchasing and Identity Theft Victimization Among Older Internet Users’ (2015) 21(7) *Psychology, Crime and Law* 681

Joyce, Daniel, ‘Privacy in the Digital Era: Human Rights Online?’ (2015) 16(1) *Melbourne Journal of International Law* 270

Kahn-Freund, Otto, ‘Blackstone’s Neglected Child: The Contract of Employment’ (1977) 93 *Law Quarterly Review* 508, 521

Kamala, Subramaniam, *Mahabharata* (Bhavan’s Book University, 19th ed, 2015)

Kluemper, Donald H, ‘Social Network Screening: Pitfalls, Possibilities, and Parallels in Employment Selection’, in Tanya Bondarouk and Miguel R Olivas-Luján (eds), *Social Media in Human Resources Management (Advanced Series in Management, Volume 12)* (Emerald Group Publishing Ltd, 2013)

Kolini, Farzan and Lech Janczewski, ‘Clustering and Topic Modelling: A New Approach for Analysis of National Cyber Security Strategies’ (Paper presented at Pacific Asia Conference on Information Systems (PACIS), Langkawi, Malaysia, 16–20 July 2017)

Korolova, Aleksandra, ‘Privacy Violations Using Microtargeted Ads: A Case Study’ (2011) 3(1) *Journal of Privacy and Confidentiality* 27

Kowalski, Robin M and Megan E Morgan, ‘Cyberbullying in Schools’ in Peter Sturmey (ed), *The Wiley Handbook of Violence and Aggression* (John Wiley & Sons, 2017) vol 3

Lapenta, Gry Hasselbalch and Rikke Frank Jørgensen, ‘Youth, Privacy and Online Media: Framing the Right to Privacy in Public Policy-Making’ (2015) 20(3) *First Monday* <http://firstmonday.org/ojs/index.php/fm/article/view/5568/4373>

Leonard, Peter, ‘An Overview of Privacy Law in Australia: Part 1’ (2014) 33(1) *Communication Law Bulletin* 1

Lopez, Ian, ‘Happy Holidays — ‘Tis the Season for Identity Theft: Consumers and Law Firms Need Increased Vigilance Against More Sophisticated Hackers’ (2015) 38(14) *National Law Journal* 18

Lowe-Calverley, Emily and Rachel Grieve, ‘Web of Deceit: Relationships Between the Dark Triad, Perceived Ability to Deceive and Cyberloafing’ (2017) 11(2) *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 5

Mair, Victor, ‘An Eighteenth-Century Version of “Liand Shanbo and Zhu Yingtai” from Suzhou’ in Victor Mair (ed), *The Columbia Anthology of Chinese Folk and Popular Literature* (Columbia University Press, 2011) 503

Malthouse, Edward C, ‘Managing Customer Relationships in the Social Media Era: Introducing the Social CRM House’ (2013) 27(4) *Journal of Interactive Marketing* 270

Mathews, Kenneth, *The New American Commentary: Genesis 1–11:26 (New American Commentary)* (B & H Publishing Group, 1996)

McCallum, Ronald and Andrew Stewart, ‘The Impact of Electronic Technology On Workplace Disputes in Australia’ (2002) 24(19) *Computer Labor Law and Policy Journal* 36

Merritt, Adrian, ‘The Historical Role of Law in the Regulation of Employment’ (1982) 1 *Australian Journal of Law and Society* 56

Milne, George R, Andrew J Rohm and Shalini Bahl, ‘Consumers’ Protection of Online Privacy and Identity’ (2004) 38(2) *Journal of Consumer Affairs* 217

Montgomery, Kathryn C, Jeff Chester and Tijana Milosevic, ‘Children’s Privacy in the Big Data Era: Research Opportunities’ (2017) 140(2) *Pediatrics*

Moskop, John C et al, ‘From Hippocrates to HIPAA: Privacy and Confidentiality in Emergency Medicine Part I: Conceptual, Moral, and Legal Foundations’ (2005) 45(1) *Annals of Emergency Medicine* 59

Mukhra, Richa et al, ‘Blue Whale Challenge: A Game or Crime?’ (2017) *Science and Engineering Ethics* 1

Ngyuen, Kenneth D, Heather Rosoff and Richard S John, 'The Effects of Attacker Identity and Individual User Characteristics on the Value of Information Privacy' (2016) 55 *Computers in Human Behaviour* 372

Nissenbaum, Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press, 2010)

Ornstein, Daniel, 'Social Media Usage in the Workplace Around the World — Developing Law and Practices' (2012) 13 *Business Law International* 195

O'Rourke, Anne and Sarah Kathryn Antioch, 'Workplace Bullying Laws in Australia — Placebo or Panacea' (2016) 45(1) *Common Law World Review* 3

Owens, Rosemary, Joellen Riley and Jill Murray, *Law of Work* (Oxford University Press, 2nd ed, 2011)

Park, Mina, Yao Sun and Margaret L McLaughlin, 'Social Media Propagation of Content Promoting Risky Health Behaviour' (2017) 20(5) *Cyberpsychology, Behaviour, and Social Networking* 278

Pattison, Michael, 'Australia' in Alan Charles Raul (ed), *Privacy, Data Protection and Cybersecurity Law Review* (Law Business Research Ltd, 2nd ed, 2015)

Pidd, Ken and Ann M Roche, 'How Effective is Drug Testing as a Workplace Safety Strategy? A Systematic Review of the Evidence' (2014) 71 *Accident Analysis and Prevention* 154

Prensky, Marc, 'Digital Natives, Digital Immigrants' (2001) 9(5) *On the Horizon* 1

Raul, Alan Charles (ed), *Privacy, Data Protection and Cybersecurity Law Review* (Law Business Research Ltd, 3rd ed, 2016)

Raul, Alan Charles (ed), *Privacy, Data Protection and Cybersecurity Law Review* (Law Business Research Ltd, 2nd ed, 2015)

Rappaport, Pauline, 'Social Media Policies and Unfair Dismissal' (2013) 18(2) *Media and Arts Law Review* 75

Reich, Warren Thomas, *Encyclopedia of Bioethics*, (Macmillan, rev. ed 1995) vol 5 (2632)

Rigoglioso, Marguerite, 'Civil Liberties and the Law in the Era of Surveillance' (2014) 49(91) *Stanford Lawyer*

Rokka, Joonas, Katariina Karlsson and Janne Tienan, 'Balancing Acts: Managing Employees and Reputation in Social Media' (2014) 30(7–8) *Journal of Marketing Management* 802

Schwartz, Baruch and Galit Caduri, 'Novelties in the Use of Social Networks by Leading Teachers in Their Classes' (2016) 102 *Computers and Education* 35

Selvadurai, Niloufer, Nazzal Kisswani and Yaser Khalaileh, 'Strengthening Data Privacy: The Obligation of Organisations to Notify Affected Individuals of Data Breaches' (2017) *International Review of Law, Computers & Technology* 1

Shakelford, Scott, Scott Russell and Andreas Kuehn, 'Unpacking the International Law on Cybersecurity Due Diligence: Lessons from Public and Private Sectors' (2016) 17(1) *Chicago Journal of International Law* 1

Sprague, Robert, ‘Invasion of the Social Networks: Blurring the Line Between Personal Life and the Employment Relationship’ (2011) 50(1) *University of Louisville Law Review* 4

Stanton, Jeffery M, ‘Traditional and Electronic Monitoring from an Organizational Justice Perspective’ (2000) 15 *Journal of Business & Psychology* 129

Svantesson, Dan Jerker B, ‘Online Workplace Surveillance — The View From Down Under’ (2012) 2(3) *International Data Privacy Law* 179–180

The Privacy Committee of New South Wales, *Drug Testing in the Workplace*, Report No 64 (1992)

Thornthwaite, Louise, ‘Social Media, Unfair Dismissal, and the Regulation of Employees’ Conduct Outside Work’ (2013) 26 *Australian Journal of Labour Law* 164

Thornthwaite, Louise, ‘Chilling Times: Labour Law and the Regulation of Social Media Policies’ (Paper presented at Labour Law Research Network Inaugural Conference, Barcelona, 13–15 June 2013)

Thornthwaite, Louise, ‘Chilling Times: Social Media Policies, Labour Law and Employment Relations’ (2016) 54 *Pacific Journal of Human Resources* 332

Thornthwaite, Louise, ‘Social Media and Work: An Emerging Privacy’ (2016) 135 *Precedent* 8

Thornthwaite, Louise, ‘Social Media and Dismissal: Towards a Reasonable Expectation of Privacy’ (2017) *Journal of Industrial Relations* 1, 3

Van der Waarden, Natalie, *Understanding Employment Law: Concepts and Cases* (LexisNexis Butterworths, 3rd ed, 2014)

Van Dissel, Beatrix M P, 'Social Media and the Employee's Right to Privacy in Australia' (2014) 4(3) *International Data Privacy Law* 222

Vass, Stephanie, 'The Anti-Social Network? Unfair Dismissal and Facebook' (2011) 2(4) *Workplace Review* 139

Vasu, Norman and Benjamin Ang, *CO16312 — Society, Technology and National Security* (23 December 2016) S Rajaratham School of International Studies, Nanyang Technological University <https://www.rsis.edu.sg/rsis-publication/cens/co16312-society-technology-and-national-security/#.Whkx90xL3BI>

Vranjes, Ivana et al, 'When Workplace Bullying Goes Online: Construction and Validation of the Inventory of Cyberbullying Act at Work (ICA-W)' (2017) *European Journal of Work and Organizational Psychology* 1

Walker, Sally, 'Lange v ABC: The High Court Rethinks the "Constitutionalisation" of Defamation Law' (1998) 5(1) *eLaw Journal: Murdoch University Electronic Journal of Law* 3 <http://www.austlii.edu.au/au/journals/MurUEJL/1998/3.html>

Warren, Samuel D, and Louis D Brandeis, 'The Right to Privacy' (1890) 4(5) *Harvard Law Review* 193

Williams, Hawys et al, ‘Dynamic Consent: A Possible Solution to Improve Patient Confidence and Trust in How Electronic Patient Records Are Used in Medical Research’ (2015) 3(1) *JMIR Medical Informatics* e3

Wilson, Nigel, ‘Regulating the Information Age — How Will We Cope With Technological Change?’ (2010) 33(2) *Australian Bar Review* 119

Wong, Paul W C, Gilbert K H Wong and Tim M H Li, ‘Suicide Communications on Facebook as a Source of Information in Suicide Research: A Case Study’ (2017) 8(1) *Suicidology Online* 1

Wright, Aliah D, *Necessary Evil: Managing Employee Activity on Facebook, LinkedIn and the Hundreds of Other Social Media Sites* (Society for Human Resource Managers, 2013)

Young, Kimberly S, ‘Internet Addiction: The Emergence of a Clinical Disorder’ (1998) 1(3) *Cyberpsychology & Behaviour* 237

B. Cases

ABC v Lenah Game Meats Pty Ltd [2001] 208 CLR 199

Appellant v Respondent (1999) 89 IR 407

Applicant v ACT Department of Education and Training [2012] FWA 2562

Application by Roberts 1 [2015] FWC 6556

Australian Postal Corporation v D’Rozario [2014] FCAFC 89

Australian Telecommunications Commission v Hart [1982] FCA 197

B, C and D v Australian Postal Corporation [2013] FWCFB 6191

Banerji v Bowles [2013] FCCA 1052 [104]

Barbulescu v Romania [2017] ECHR 754

Blyth Chemicals v Bushnell (1933) 49 CLR 66

Bray v Ford [1896] AC 44

Brown v Woolworths Ltd PR 958576 [2005] AIRC

Byrne v Australian Airline (1995) 185 CLR 410

CFMEU v Hail Creek Coal Pty Ltd [2016] FCA 1032

*City of Ontario v Quon 130 (*2010) S Ct 2619

Clarkin v Bechtel Construction (Australia) Pty Ltd [2017] FWC 1871

Colakovski v Australian Telecommunications Corporation (1991) 100 ALR 111

Commonwealth Bank of Australia v Barker (2014) 253 CLR 169

Concut Pty Ltd v Worrell (2000) 176 ALR 693

Construction, Forestry, Mining and Energy Union — Construction and General Division v Port Kembla Coal Terminal (PKCT) [2015] FWCFB 4075

Dekort v Johns River Tavern Pty Ltd [2010]

Dover-Ray v Real Insurance Pty (2010) 204 IR 399

Dover-Ray v Real Insurance Pty Ltd (2010) FWA 8544

Edwards v Guidice [1999] FCA 1836 4, 6–7

Faccenda Chicken Ltd v Fowler [1986] 1 All ER 617

Fallens v Serco Australia Pty Ltd [2015] FWC 8394

Fitzgerald v Smith [2010] FWA 7358

Griffiths v Rose (2011) 192 FCR 130

Harbour City Ferries Pty Ltd v Toms [2014] FWCFB 6249

Harmer v Cornelius (1858) 5 CNBC 236

Hodgson v Amcor [2012] VSC 94

Jones v Queensland Tertiary Admissions Centre Ltd (No 2) (2010) FCA 339

Jurecek v Director of Transport Safety Victoria [2016] VSC 285

Katz v United States 39 US 347 (1967)

Lange v Australian Broadcasting Corporation (1997) 189 CLR 520

Laws v London [1959] 1 WLR 698 CA 700

Linfox Australia Pty Ltd v Stutsel [2012] FWAFB 7097

Linfox Australia Pty Ltd v Fair Work Commission and Stutsel [2013] FCAFC 157

Lister v Romford Ice and Cold Storage Co Ltd [1957] AC 555

Little v Credit Corporation Group Ltd [2013] FWC 9642

Mahmud v Bank of Credit and Commerce International SA [1998] AC 20

Maximillian Schrems v Data Protection Commissioner (Court of Justice of the European Union, C-362/14, 6 October 2015)

Mayberry v Kijani Investments Pty Ltd ATF The Dawe Investments Trust Subway Wallsend [2011] FWA 3496

McDonald v South Australia; McDonald v Minister for Education and Child Development [2017] SASCFC 146

McIntyre v Special Broadcasting Services Corporation [2015] FWC 6768

McManus v Scott-Charlton (1996) 70 FCR 16

Millar v Taylor (1769) 98 ER 201

Ms SB [2014] FWC 2104

Neat Holdings Pty Ltd v Karajan Holdings Pty Ltd (1992) HC 67 ALJR 170

NSW AG Department v Miller [2007] NSWIRComm 33 [113]–[123]

O'Connor v Outdoor Creations Pty Ltd [2011] FWA 3081

O'Keefe v William Muir's Pty Ltd [2011] FWA 5311

Owen Sharp v BCS Infrastructure Support Pty Ltd [2015] FWCFB 1033

Orr v University of Tasmania (1957) 100 CLR 526

Parmalat Food Products Pty Ltd v Wililo [2011] FWAFB 1166

Pearse v Viva Energy Refining Pty Ltd [2017] FWCFB 4701

Pearson v Linfox Australia Pty Ltd [2014] FWC 446

Pearson v Linfox Australia Pty Ltd [2014] FWCFB 1870

Pedley v IPMS Pty Ltd [2013] FWC 4282

Privacy Commissioner v Telstra Corporation Ltd [2017] FCAFC 4

Re Ms SW [2014] FWC 3288

Rose v Telstra Corporation Ltd [1998] AIRC 1592

Selvachandran v Peteron Plastics Pty Ltd (1995) 62 IR 371 [373] reg 1.07 Fair Work Regulations 2009 (Cth)

Smith v Fitzgerald [2011] FWAFB 1422

Solibrooke Pty Ltd v Vosper [2016] FWCFB 2421

South Australia v McDonald (2009) 104 SASR 344

Starr v Department of Human Services [2016] FWC 1460

Stutsel v Linfox Australia Pty Ltd [2011] FWA 8444

Tao Sun [2014] FWC 3839

Toms v Harbour City Ferries Pty Ltd [2014] FWC 2327

Tran v Callum Textiles Pty Ltd (1997) 42 AILR 3-553 (No VI 1401 of 1996)

Vestergaard Frandsen A/S v Bestnet Europe Ltd [2013] UKSC 31

Vosper v Solibrooke Pty Ltd [2016] FWC 1168

Wilkinson-Reed v Launtoy Pty Ltd [2014] FWC 644

Willmott v Woolworths Ltd [2014] QCAT 601

Wilson v Ferguson [2015] WASC 15

Woolworths Ltd v Brown PR 963023

C. Legislation

Anti-Discrimination Act 1991 (Qld)

Age Discrimination Act 2004 (Cth)

Australian Constitution

Australian Human Rights Commission Act 1986 (Cth)

Bundesdatenschutzgesetz [Federal Data Protection Act] (Germany) 14 August 2009, BDSG, 2009, 2814

Civil Rights Act 1964 (USA)

Council Directive 95/46/EC of the European Parliament and of the Council of the 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31

Crimes Amendment (Intimate Images) Act (NSW)

Disability Discrimination Act 1992 (Cth)

Fair Work Act 2009 (Cth)

Freedom of Information Act 1982 (Cth)

Freedom of Information Amendment (Reform) Act 2010 (Cth)

Human Rights Act 1989 (UK)

Industrial Relations Act 1979 (WA)

Privacy Act 1988 (Cth)

Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)

Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)

Racial Discrimination Act 1975 (Cth)

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L 8/1

Sex Discrimination Act 1984 (Cth)

Summary Offences Act 1966 (Vic)

Summary Offences (Filming and Sexting Offences) Amendment Act 2016 (SA)

Telecommunications (Interception and Access) Act 1979 (Cth)

Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Cth)

D. Treaties

European Convention on Human Rights

E. Other

9News, *Nurses Removed From Duty After Making Newborn Dance for Video* (20 September 2017) <http://www.9news.com.au/world/2017/09/20/07/54/nurses-removed-from-duty-after-making-newborn-dance-for-video>

Angwin, Julia, 'The Web's New Gold Mine: Your Secrets', *Wall Street Journal* (online), 30 July 2010 <https://www.wsj.com/articles/SB10001424052748703940904575395073512989404>

Apple Inc, *A Bold Way To Look at Your Health* (2017) <https://www.apple.com/au/ios/health/>

Apple Inc, *iCloud Security Overview* (7 November 2017) <https://support.apple.com/en-sg/HT202303>

AppleInsider Staff, *Apple Music Passes 11M Subscribers and iCloud Hits 782M Users* (12 February 2016) AppleInsider <http://appleinsider.com/articles/16/02/12/apple-music-passes-11m-subscribers-as-icloud-hits-782m-users>

Arnold, Bruce Baer, 'Care Don't Share: What Medvet Breach Says About Australian Privacy Laws', *The Conversation*, 8 August 2011 <http://theconversation.com/care-dont-share-what-medvet-breach-says-about-australian-privacy-laws-2594>

Australian Bureau of Statistics, *8146.0 — Household Use of Information Technology, Australia, 2012–13: Patterns of Home Internet Use* (25 February 2014) <http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/8A12E6E0D07D36A0CA257C89000E3FB7>

Australian Bureau of Statistics, *8146.0 — Household Use of Information Technology, Australia, 2010-11: Personal Internet Use* (15 December 2011) <http://www.abs.gov.au/ausstats/abs@.nsf/0/D11394A54F8B9ED1CA25796600152C62>

Australian Human Rights Commission, *A Quick Guide to Australian Discrimination Laws* (October 2016) <https://www.humanrights.gov.au/employers/good-practice-good-business-factsheets/quick-guide-australian-discrimination-laws>

British Standards Institution, *BS 7858:2012 Security Screening of Individuals Employed in a Security Environment. Code of Practice* (31 October 2012) <https://shop.bsigroup.com/ProductDetail?pid=000000000030237324>

Cambridge Dictionary, (2018) accessed 17 January 2018

Carlson, Nicholas, 'Larry Page Just Tied ALL Employees' Bonuses to the Success of Google's Social Strategy', *Business Insider* (online), 7 April 2011 <http://www.businessinsider.com/larry-page-just-tied-employee-bonuses-to-the-success-of-the-googles-social-strategy-2011-4>

Centre for the Protection of National Infrastructure, *Pre-Employment Screening: A Good Practice Guide* (5th ed, 2015) <https://www.cpni.gov.uk/system/files/documents/61/e9/pre-employment-screening-A-good-practice-guide-edition-5.pdf>

Hern, Alex, 'Former Microsoft employee arrested over Windows 8 leaks', *The Guardian (International Edition)* (online), 20 March 2014 10.49 GMT <https://www.theguardian.com/technology/2014/mar/20/former-microsoft-employee-arrested-over-windows-8-leaks>

Chabad Sola – South Cienega, CA (Jewish.tv) Home page, Talmud, Bava Metzia 113, Video, 8:35–49.16 <http://dot_net-origin.chabad.org/dailystudy/talmud_cdo/aid/3446486/jewish/Talmud-Bava-Metzia-113.htm>

Christensson, P, 'Metadata' (2006) *TechTerms* <https://techterms.com/definition/metadata>

Commonwealth Bank of Australia, *CBA Social Media Policy* (1 December 2010) <https://www.google.com.au/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiW7ZiZ8cnXAhUCy7wKHRuXCTkQFggoMAA&url=http%3A%2F%2Fcommetrics.com%2Fdownload%2F37%2F&usg=AOvVaw1QPkYpp3H4Oa-JV0u0wTJB>

Court of Justice of the European Union, 'The Court of Justice Declares that the Commission's US Safe Harbour Decision is Invalid' (Press Release, 117/15, 6 October 2015)

Cox, Noel 'Constitutional Responses to Paradigmatic Shifts in Technology' pg 6 June 2008 (updated / as at 17 October 2017) SSRN Electronic Journal DOI10.2139/ssrn.1140464 <https://www.researchgate.net/publication/228233694_Constitutional_Responses_to_Paradigmatic_Shifts_in_Technology>

Cross-tab, 'Online Reputation in a Connected World' (27 January 2010) <download.microsoft.com/.../dpd_online%20reputation%20research_overview.doc> Accessed on 17 January 2018 Alternative site: Braak, Nick, 'Online Reputation in a Connected World' LinkedIn Slideshare 27 January 2010 <https://www.slideshare.net/nickbraak/online-reputation-in-a-connected-world>

Department of Education and Training, The Department, (accessed 14 November 2017) <https://www.education.gov.au>

Department of Education and Training, *Privacy Policy* (accessed 9 August 2017) <https://www.education.gov.au/privacy-policy>

Homepage Australian Government Department of Education and Training, *The Department* (Accessed 17 January 2018) <https://www.education.gov.au/department>

Dharshini, Mary Pascaline, 'Vitality: Internet Addiction May Lead To More Mental Health Problems Study Finds', *Medical Daily* (online), 19 September 2016 <http://www.medicaldaily.com/internet-addiction-internet-usage-mental-health-depression-and-anxiety-398216>

Dunbar, Robin, *How Many Friends Does One Person Need? Dunbar's Number and Other Evolutionary Quirks* (Harvard University Press, 2010)

Dunbar, Robin, 'You've Got to Have (150) Friends', *New York Times* (online), 25 December 2010 <http://www.nytimes.com/2010/12/26/opinion/26dunbar.html>

European Commission, *Communication from the Commission to the European Parliament and the Council: Rebuilding Trust in EU–US Data Flows* (27 November 2013) <http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf>

European Union Agency for Fundamental Rights, *Data Protection* (2017) <http://fra.europa.eu/en/data-protection>

European Union Agency for Law Enforcement, 'How To Set Your Privacy Settings on Social Media', *Europol* (Accessed 17 January 2018) <https://www.europol.europa.eu/how-to-set-your-privacy-settings-social-media>

Explanatory Memorandum, Fair Work Bill 2008 (Cth)

Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth)

Facebook, *Company Info-Stats* (2017) Facebook Newsroom <https://newsroom.fb.com/company-info/>

Federal Trade Commission, *Privacy Enforcement and Safe Harbor: Comments of FTC Staff to European Commission Review of the US–EU Safe Harbor Framework* (12 November 2013) <https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-enforcement-safe-harbor-comments-ftc-staff-european-commission-review-u.s.eu-safe-harbor-framework/131112europeancommissionsafeharbor.pdf>

Fitbit Inc, *How Do I Connect With Friends With Fitbit?* (2017) <https://help.fitbit.com/articles/en_US/Help_article/1858>

Flannery, Angela, *Grubb's Case and the Meaning of Personal Information* (3 March 2017) Mondaq <http://www.mondaq.com/australia/x/573252/Data+Protection+Privacy/Grubbs+case+and+the+meaning+of+personal+information>

Friedman, Lindsay, *The 12 Worst Social-Media Fails of 2016* (22 September 2016) Entrepreneur <https://www.entrepreneur.com/slideshow/272286#0>

Harben, Saul and Steve Bowler, *Drug and Alcohol Use: When Zero Tolerance is Tolerable* (2 April 2015) Clayton Utz <https://www.claytonutz.com/knowledge/2015/april/drug-and-alcohol-use-when-zero-tolerance-is-tolerable>

Harrel, Erika, *Victims of Identity Theft, 2014* (27 September 2015) Bureau of Justice Statistics <https://www.bjs.gov/index.cfm?ty=pbdetail&iid=5408>

Hern, Alex, 'Windows 10: Microsoft Under Attack Over Privacy', *Guardian* (online) 1 August 2015 <https://www.theguardian.com/technology/2015/jul/31/windows-10-microsoft-faces-criticism-over-privacy-default-settings>

Homepage Instagram, https://www.instagram.com Accessed 17 January 2018

Homepage, WhatsApp Inc, <https://www.whatsapp.com> (Accessed 17 January 2018)

Homepage, End-to-End Encryption (2018) WhatsApp Inc, WhatsApp Web <https://faq.whatsapp.com/en/general/28030015> (Accessed 17 January 2018)

Israel Internet Association, *That's How the Internet Looks to Your Children,* <https://www.isoc.org.il/sts-data/23150>

Israeli Ministry of Education, *Director General Communication, Instruction 9.4–1: Education to Protectedness, to Ethic Keeping and to Appropriate and Wise Behaviour on the Web* [In Hebrew] < ttps://www.researchgate.net/publication/264821418_Student-teacher_relationship_in_the_Facebook_era_the_student_perspective> Accessed 17 January 2018

KPMG, *Process Review of Fair Work Australia's Investigations into the Health Services Union* (17 August 2012) Fair Work Commission

<https://www.fwc.gov.au/documents/documents/organisations/reports/kpmg_review.pdf>

Kroll Intelligence Center, *Cyber Due Diligence: Pre-Transaction Assessments Can Uncover Costly Risks* (28 January 2015) <http://blog.kroll.com/2015/cyber-due-diligence-pre-transaction-assessments-can-uncover-costly-risks/>

Lavoipierre, Angela, 'National Revenge Porn Legislation to Impose Fines for Abusers Slated for this Year' *ABC News* (online), 10 November 2017 <http://www.abc.net.au/news/2017-11-10/new-revenge-porn-legislation-to-impose-civil-penalties/9138040>

Lord, Nate, 'What is Data Encryption?' on *Data Insider* (27 July 2017) <https://digitalguardian.com/blog/what-data-encryption>

Lum, Selina, 'S'porean Fugitive Lived a Lie in US as a "Lawyer" for Years', *Straits Times* (online), 19 May 2016 <http://www.straitstimes.com/singapore/courts-crime/sporean-fugitive-lived-a-lie-in-us-as-lawyer-for-years>

Merriam-Webster Dictionary, <https://www.merriam-webster.com/dictionary/anarchy>

Meyer, David, 'Here's Why France's Demands Could Hammer Facebook's Business Model', *Fortune,* 9 February 2016 <http://fortune.com/2016/02/09/france-facebook-advertising/>

Meyer, David, ‘Belgian Police Say Facebook Reactions Could Be Dangerous’, *Time* (online), 12 May 2016 <http://time.com/4327641/belgian-police-facebook-reactions-dangerous>

Newman, Rima, Kristopher Cook and Zoe Brick, ‘The Risks of Using Social Media to Screen Job Candidates’, *Lexology*, 17 May 2016 <https://www.lexology.com/library/detail.aspx?g=5e6172ce-f5f5-471a-ab1f-2a6f12ff0ca4>

Office of the Information Commissioner, *Chapter 1: APP 12.1 — Open and Transparent Management of Personal Information* (February 2014) <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-1-app-1-open-and-transparent-management-of-personal-information>

Pelish, Jason, ‘10 Different Types of Fake Facebook Accounts’ on Jason Pelish, *The Click Whisperer* (4 April 2014) <https://www.clickwhisperer.com/2014/04/04/the-10-types-of-fake-facebook-accounts/>

Pilcher, Jeffry, ‘Bank’s Social Media Policy Says Snitch & Spy on Your Friends or You’re Fired’, *The Financial Brand,* 7 February 2011 <https://thefinancialbrand.com/16718/commonwealth-bank-social-media-policy/>

Pilgrim, Timothy, ‘The Value of Public Sector Information’ (Speech delivered at the AGS FOI and Privacy Forum, Canberra, 4 May 2016) <https://www.oaic.gov.au/media-and-speeches/speeches/the-value-of-public-sector-information>

Pipl, Home page <https://pipl.com>

Ritualize, Home page <https://ritualize.com/main/?>

Powering Employee Engagement – Investing in your employees health and well-being is really an investment in your company's bottom line> *Homepage, Wellteq* <wellteq.co> (Accessed 17 January 2018) and previously known as Globetrekker, <http://www.globetrekkerchallenge.com>

Press Trust of India, 'Corporate Business Secrets Getting Leaked on Social Media Websites', *Economic Times* (online), 21 November 2011 <https://economictimes.indiatimes.com/tech/internet/corporate-business-secrets-getting-leaked-on-social-media-websites/articleshow/10816341.cms>

Price, David, *How to Use iCloud* (16 May 2017) Macworld <https://www.macworld.co.uk/how-to/mac-software/how-use-icloud-3659150/>

PrivacyTrust, *PrivacyTrust Safe Harbor Program*, <https://www.privacytrust.com/safeharbor/>

Quran Al-Nur, 24:27–28 < https://quran.com/24/27-28> Accessed 17 January 2018.

Rouse, Margaret, *Metadata* (July 2014) TechTarget <http://whatis.techtarget.com/definition/metadata> Accessed 17 January 2018

Ryoo, Jungwoo, 'Big Data Security Problems Threaten Consumers' Privacy', *The Conversation*, 23 March 2016 <https://theconversation.com/big-data-security-problems-threaten-consumers-privacy-54798>

Schmidt, Eric, as quoted by Saxon R Shaw, ‘There is No Silver Bullet: Solutions to Internet Jurisdiction’ (2017) *International Journal of Law and Information Technology* 1–26

Snap Inc, Home page, <https://www.snapchat.com>

Sun, Carolyn, ‘These Social Media Fails Got People Fired’, *Entrepreneur*, 18 March 2016 <https://www.entrepreneur.com/article/271823>

Trindale, Dan, ‘Employees’ Duty to Report Misconduct of Themselves or Others’ on Clayton Utz, *Knowledge* (26 April 2012) <https://www.claytonutz.com/knowledge/2012/april/employees-duty-to-report-misconduct-of-themselves-or-others>

United States Department of Justice, *Child Pornography* (25 July 2017) <https://www.justice.gov/criminal-ceos/child-pornography>

Van den Hoven, Jeroen et al, ‘Privacy and Information Technology’ *Stanford Encyclopedia of Philosophy Archive* (online, 21 March 2016) <https://plato.stanford.edu/archives/win2014/entries/it-privacy/>

Wood, Sally, ‘Statistics for Social Media Usage in Australia: What They Mean for Your Online Marketing Efforts’, *Marketing.com.au*, 3 July 2015 <https://marketing.com.au/statistics-for-social-media-usage-in-australia/>

Yadron, Danny, ‘Edward Snowden: “I’m Not an Unhappy Ending” for Future Whistleblowers’, *Guardian* (online), 3 April 2016 <https://www.theguardian.com/us-news/2016/apr/01/edward-snowden-whistleblower-russia-exile>

Zuckerberg, Mark, *Building Global Community* (17 February 2017) Facebook <https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10154544292806634>