PRIVACY CONCERNS OVER EMPLOYER ACCESS TO EMPLOYEE SOCIAL MEDIA

MURRAY BROWN* AND CHRIS DENT**

Amid increasing concerns about the encroachment of work on private life, this article examines the extent to which Australian employers should be able to access their employees' personal social media posts, with specific reference to ongoing surveillance and the forced disclosure of passwords. Both the federal workplace and privacy legislation are discussed to consider the extent to which they offer appropriate protections. Given their limitations, other options, including a tort of privacy and a workplace privacy regulator, are raised that may better protect the privacy and freedom of expression of employees. Black's notion of 'decentred regulation' is applied to the current, and proposed, law in order to better understand the positives, and negatives, of the legal controls over employer access to the social media of their employees.

I INTRODUCTION

'Social media' is an umbrella term for various websites that integrate technology, user-generated content and social interaction. These sites generally allow users to create, download and share content, publish a profile and other personal information, and connect with others.[1] Social media use is verging on the ubiquitous in Australia. There were, for example, 13 million active Facebook users each month in 2015.[2] There are other more specialised social media sites. Twitter is aimed at the communication of 140 character-long messages as contributions to debate (via hashtags) or to 'followers'. Tinder and Grindr facilitate 'hook-ups'

* School of Law, Murdoch University. This article was begun while the author was on sabbatical at Jesus College, Cambridge in 2013. I would like to thank the Fellows of the College for their very generous hospitality. I would like to particularly thank Mr Christopher Pratt. I would also like to thank the participants of a seminar at the Cambridge Private Law Centre in November 2013 for their comments on an early draft of the paper. I would like to especially thank the two co-convenors of the seminar, Dr David Erdos and Dr Kirsty Hughes. Thanks are also due to Dr Normann Witzleb and Natalie van der Waarden for their comments on later drafts of the paper. My co-author and I naturally remain responsible for any errors.

** Associate Professor, School of Law, Murdoch University. In the interests of full disclosure, I was a researcher and a co-author for the Victorian Law Reform Commission's *Workplace Privacy*, Issues Paper (2002). I, however, had no separate input into its Final Report for the reference.

1 Eugenia Siapera, *Understanding New Media* (Sage Publications, 2012) 202.

2 Alex Heber, 'These Incredible Stats Show Exactly How Huge Facebook Is in Australia', *Business Insider Australia* (online), 8 April 2015 <http://www.businessinsider.com.au/these-incredible-stats-show-exactly-how-huge-facebook-is-in-australia-2015-4>.

and other forms of 'social discovery'.[3] Most forms of social media, therefore, are based on the idea that users will upload information about themselves in order to participate in a community.[4] As such, they can be seen as a reflection of a basic human desire — with such expression being 'an integral aspect of each individual's right to self-development … [that] instantiates or reflects what it is to be human'.[5]

This brave new world poses a challenge for the law in many respects.[6] This article focuses on the extent to which employers should be able to access their employees' personal social media posts and in particular monitor social media for postings by their employees outside of working hours or require the disclosure of passwords. More specifically, social media has allowed employers unprecedented access to what would, at least once, have been considered their employees' private lives. The speed of this change is also unprecedented — just over a decade ago, the Victorian Law Reform Commission ('VLRC') released a report on workplace privacy, without a single reference to 'social media'.[7] Since then, there have been a number of Australian cases that have dealt with dismissals on the basis of social media posts,[8] as well as suggestions that the availability of new technology and services to employers is leading to increased monitoring of employee online behaviour.[9] That both workplace and privacy law are engaged supports the approach taken in this article — the adoption of a higher level, regulatory approach that privileges neither of the two bodies of law. Expressed differently, it is not clear that either the employee, or the employer, considers their actions in terms of the strict legal categories; as such, a more inclusive approach is warranted. Using insights from regulatory theory, therefore, provides a broader perspective on, and the possible solutions to, the issue.

3 Stuart Dredge, 'Tinder: The "Painfully Honest" Dating App with Wider Social Ambitions', *The Guardian* (online), 25 February 2014 <http://www.theguardian.com/technology/2014/feb/24/tinder-dating-app-social-networks>.

4 One of the claimed benefits of social media is that it has helped people worldwide, including those who might otherwise have been outcasts, link to others with common interests for conversation and support. Survey results show too that '[m]embers of online groups … say the Internet brings them into more contact with people outside their social class or their racial or age group': Leigh A Clark and Sherry J Roberts, 'Employer's Use of Social Networking Sites: A Socially Irresponsible Practice' (2010) 95 *Journal of Business Ethics* 507, 515.

5 Eric Barendt, *Freedom of Speech* (Oxford University Press, 2nd ed, 2005) 13.

6 An obvious example is defamation: see, eg, *Mickle v Farley* (2013) 18 DCLR (NSW) 51.

7 VLRC, *Workplace Privacy*, Final Report (2005). Unsurprisingly, there was also no mention of 'social media' in the earlier publication: Ronald McCallum, *Employer Controls Over Private Life* (University of New South Wales Press, 2000). For a more recent discussion of workplace privacy, see Normann Witzleb, 'Employee Monitoring and Surveillance under Australian Law: The Need for Workplace Privacy Legislation' in Dieter Dörr and Russell L Weaver (eds), *Perspectives on Privacy: Increasing Regulation in the USA, Canada, Australia and European Countries* (De Gruyter, 2014) 126.

8 The case law will be referred to in the analysis below.

9 Gartner, 'Gartner Says Monitoring Employee Behavior in Digital Environments is Rising' (Press Release, 29 May 2012) <http://www.gartner.com/newsroom/id/2028215>.

II COMPLEXITIES AROUND EMPLOYER ACCESS TO EMPLOYEE SOCIAL MEDIA

It is not contentious or unusual to consider that social media has privacy implications.[10] On opening a Facebook account, for example, a new user is prompted to provide as many as 40 items of information for his or her profile including their 'name; birthday; political and religious views; … sexual preference, and relationship status; … educational and employment history' and a photograph.[11] Like many other sites, such as Instagram, Facebook also allows users to upload pictures and videos to their personal web page, as well as post messages. Further, users of these platforms may 'tag' their photos in a way that identifies the other people in the picture by name — providing online links that are created without the explicit consent of both parties.[12] The issue to be addressed in this Part is the extent of the complexities involved when social media posts are considered in the context of work.

A *Competing Tensions Relating to Employer Access*

This section highlights a number of the tensions that impact on any attempt to regulate social media. One of these has general relevance, while some are most specific to the employer-employee relationship.[13] The general binary is the distinction between what happens online and what happens in the 'real' world. The reach of communications is much broader in the former than in the latter.[14] This is an obvious point, but one that needs to at least be referred to. If, for example, a Twitter user sends a message to a Q&A debate on television — an action that has been judicially likened to 'scream[ing] … out the window'[15] — then they would have a greater audience than if they spoke the comment aloud in their lounge-room. That said, there is the greater potential for anonymity in

10 There is also not the space to justify privacy as something that needs to be protected. This article assumes that privacy is a 'good' valued by most people — though the precise boundaries of what is considered 'private' varies from individual to individual and is dependent upon the circumstances in which that privacy may be negatived.

11 James Grimmelmann, 'Saving Facebook' (2009) 94 *Iowa Law Review* 1137, 1149.

12 Despite changes on Facebook that allow members to approve or delete a tag before it is posted to their page, 'the ultimate control lies with the third party who posted the content. … There, depending on your friend's privacy settings, it could potentially be viewed by your friend's friends or by further third parties. If the friend in question does not remove the tag then the user may defriend or block them, yet the photograph will remain "out there" in the social network in perpetuity': Natasha Simmons, 'Facebook and the Privacy Frontier' (2012) 33 *Business Law Review* 58, 59.

13 The analysis here, therefore, is based on the existence of an employment relationship. On whether Australian law allows employers to screen job applicants via social media, see Murray Brown, 'Applying for a Job with Big Brother: Is Online Vetting of Job Applicants Lawful in Australia?' (2012) 37 *Alternative Law Journal* 186.

14 In the words of a US court, loading material online makes the work 'available to any person with a computer and thus open[s] it to the public eye. … [The] potential audience [is] vast': *Moreno v Hanford Sentinel Inc*, 91 Cal Rptr 3d 858, 862–3 [7]–[8] (Ct App, 2009).

15 *People v Harris*, 949 NYS 2d 590, 595 (Crim Ct, 2012).

expression in online communications than there is in face-to-face public debate.[16] On the other hand, there are some suggestions that the expectations of the off-line world are to be found online. It has, for example, been argued that users of social media sites have developed a new concept of privacy ('network privacy') 'based on the expected accessibility of personal information to social constituencies'.[17] Users, they suggest, demand 'the ability to create distinct personae, … to sustain "firewalls" between social, work, and familial groups'[18] — something which most of us do routinely in our off-line lives, at least to some extent.

In addition to this, there are three binaries of relevance to the employer-employee relationship, that need to be raised here. The first of these is the obvious one — the tension between an employee's role as a worker and their role outside work. For employees, there is a need to keep the two separated. In simple terms, users expect employers to refrain from accessing or judging them on the basis of information intended for another audience, such as their friends or broader peer group. Davis captures the sentiment well:

> Members of Generation Y do not consider their online profiles the province of their employer much in the same way an older generation would think it improper and invasive for an employer to show up at an employee's private party unannounced.[19]

This has been explored empirically. A survey of 2 500 users of social networking sites aged between 18 and 24 suggested that, even though users of these sites disclose a high degree of personal information online, they retain an expectation of privacy, especially vis-à-vis employers.[20] Those surveyed were asked to respond to various scenarios, including one in which an employer accessed information not intended for them. Fifty four per cent of respondents 'believed … it … wrong for people to access information … not intended for them',[21] while a similar percentage agreed with the statement, '[w]ork life is completely separate from personal life, and what you do in one should not affect the other'.[22] In another analysis, 75 per cent of respondents thought it inappropriate for a manager to use a social network site to see what employees are doing during their personal time, without them knowing.[23] Or, as has been stated — 'an employee is "entitled to a private life"'.[24]

16 As an example of a workplace case based on 'anonymous' tweets, see *Banerji v Bowles* [2013] FCCA 1052 (9 August 2013).

17 Avner Levin and Patricia Sánchez Abril, 'Two Notions of Privacy Online' (2009) 11 *Vanderbilt Journal of Entertainment and Technology Law* 1001, 1045.

18 Ibid.

19 Donald Carrington Davis, 'MySpace Isn't Your Space: Expanding the *Fair Credit Reporting Act* to Ensure Accountability and Fairness in Employer Searches of Online Social Networking Services' (2006) 16 *Kansas Journal of Law & Public Policy* 237, 240.

20 Levin and Abril, above n 17, 1004.

21 Ibid 1026.

22 Ibid 1043.

23 Patricia Sánchez Abril, Avner Levin and Alissa Del Riego, 'Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee' (2012) 49 *American Business Law Journal* 63, 100.

24 Louise Thornthwaite, 'Social Media, Unfair Dismissal and the Regulation of Employees' Conduct Outside Work' (2013) 26 *Australian Journal of Labour Law* 164, 170, quoting *Rose v Telstra* [1998] AIRC 1592 (4 December 1998).

The second tension relates to the extent to which social media posts may impact on the employer. Of course, any post is not going to directly cause physical harm to the employer or the business; however, comments by an employee may lead to financial damage — including, but not limited to, a downturn in custom (if the posts are to damage reputation) or the loss of trade secrets. The potential for a post to have an adverse impact may depend on the position the employee has in the company,[25] the duration that the post is visible, the potential audience of the post, whether the post contains confidential information and, of course, the severity of the comments.[26] As has been said, '[a]n employee has a right to complain about their employment rights and their treatment at work', but that is not allowed to extend to damaging the reputation or financial health of the employer.[27] Self-expression is a key interest of those who use social media; employers — whether they be private or public organisations[28] — have an interest in maintaining their profile in society or the economy.

The third tension concerns the purpose of any access by an employer of an employee's social media posts. An employer may seek access in order to investigate an alleged incident at work. Alternatively, an employer may engage in ongoing surveillance of social media to protect against potential harm that the employer considers the employee may commit. This might be confined to surveillance of high-risk employees but could potentially extend to routine surveillance of all employees. There is certainly the capacity for employers to continually monitor employee social media for problematic (in the eyes of the employer at least) posts. As long ago as 2010, for example, 'Social Sentry' was released — a product that was claimed to be capable of automatically detecting any employee posting on Facebook as well as some other social media sites, even where a pseudonym was used, for as little as US$2 per employee.[29] Any such surveillance has the potential to have a chilling effect on the behaviour of individuals who are aware that they are under surveillance, even if no information is actually collected.

Where a specific incident is being investigated, employer access to a worker's social media posts can be as simple as the employer searching for the employee on the internet. Non-private Facebook pages may come up, as may LinkedIn pages. Arguably, the latter are less of a concern with respect to privacy, as these pages are often set up with the employment context in mind. Some US legal commentators have argued, on the other hand, that employer checks of even public social media pages may violate privacy rights, at least if performed without the employee's

25 Thornthwaite, for example, raises the special circumstances of teachers: Thornthwaite, 'Social Media, Unfair Dismissal and the Regulation of Employees' Conduct Outside Work', above n 24, 174.

26 See, eg, the discussion in *Stutsel v Linfox Australia Pty Ltd* (2011) 217 IR 28.

27 *Vosper v Solibrooke Pty Ltd* [2016] FWC 1168 (1 March 2016) [20].

28 The reputation of a government department was highlighted in *Starr v Department of Human Services* [2016] FWC 1460 (29 March 2016). This case was discussed in Louise Thornthwaite, 'Social Media and Work: An Emerging Privacy' [2016] (135) *Precedent* 8.

29 Joshua Brustein, 'Keeping a Closer Eye on Employees' Social Networking', *The New York Times* (online), 26 March 2010 <http://bits.blogs.nytimes.com/2010/03/26/keeping-a-closer-eye-on-workers-social-networking>.

knowledge or consent.[30] Indeed, Sprague suggests that it 'is tantamount to electronic eavesdropping' for an employer to view an employee's public social media site, if the information on those pages had only been intended to be shared with a few friends.[31] Where private social media pages are concerned, the information, or even a password may come from another worker. The outcome of the UK Employment Tribunal decision of *Crisp v Apple Retail (UK) Ltd*[32] shows that the Tribunal did not think that the handing over of the content of a private post, without the consent of the employee who made the problematic post, was a serious enough issue to hold the dismissal to be unfair. One of the Australian cases that have raised the issue, *Wilkinson-Reed v Launtoy Pty Ltd*,[33] while finding that the dismissal in question was unfair, did not discuss the ramifications of how the password was obtained. In another decision, the Fair Work Commission ('FWC') stated that gaining a Facebook password from an ex-partner of the employee was 'inappropriate'.[34]

An investigation, therefore, may require access to a password. The most problematic way for an employer to obtain that password is through demanding it — either directly from the employee concerned or from a co-worker of the employee. An example of the latter instance is the US case involving Brian Pietrylo.[35] He had created a password-protected MySpace page and invited his fellow restaurant employees to join and 'talk about all the crap/drama/and gossip occurring in our workplace, without hav[ing] to worry about outside eyes prying'.[36] Members of the group made sexual comments about management and customers, joked about customer service and made reference to violence and illegal drug use. Management became aware of the site and gained access to it by asking another employee, St Jean, for her password. It then dismissed Pietrylo, who responded by suing the restaurant. On appeal, it was held that, in light of St Jean's evidence at trial that she had only provided her password to management because she felt that otherwise she probably 'would have gotten in some sort of trouble', the jury had reasonably concluded that the restaurant's access to the MySpace page was not authorised under the federal *Stored Communications Act* 18 USC § 2701.[37]

30 Carolyn Elefant, 'The "Power" of Social Media: Legal Issues & Best Practices for Utilities Engaging Social Media' (2011) 32 *Energy Law Journal* 1, 14 n 60.

31 Robert Sprague, 'Rethinking Information Privacy in an Age of Online Transparency' (2008) 25 *Hofstra Labor & Employment Law Journal* 395, 410.

32 (Unreported, Employment Tribunals, Oliver J, 5 August 2011).

33 [2014] FWC 644 (24 January 2014).

34 *Fallens v Serco Australia Pty Ltd* [2015] FWC 8394 (3 December 2015) [20]. The Commissioner also said that they were 'satisfied on the balance of probabilities that the private Facebook conversations were obtained in breach' of s 440 of the *Criminal Code Act Compilation Act 1913* (WA) — though this finding had no impact on the orders of the Commission.

35 For a more complete review of the US law in the area, see Louise Thornthwaite, 'Chilling Times: Social Media Policies, Labour Law and Employment Relations' (2016) 54 *Asia Pacific Journal of Human Resources* 332.

36 *Pietrylo v Hillstone Restaurant Group* (D NJ, Civ No 06-CV5754 (FSH), 7 September 2007) slip op 3.

37 *Pietrylo v Hillstone Restaurant Group* (D NJ, Civ No 06-5754 (FSH), 25 July 2008) slip op 1 (Hochberg J).

While not dealing precisely with the circumstances in the *Pietrylo* case, a number of US states have passed laws prohibiting employers from asking job applicants or employees to disclose their username, password, or other information needed to access a personal social media account. The legislation in most states goes beyond merely prohibiting requests for log-in information. One of the broadest prohibitions is found in the Vermont legislation, which also prohibits an employer from requesting an employee to 'access a social media account[38] in [their] presence …; divulge … any content from [that account]; … change [its] privacy settings … to increase third-party access to its contents … [or] add anyone … to [the] list of contacts associated with [the] account'.[39]

However, most US states also have an exception for workplace investigations. For example, the Michigan legislation provides that it does not prohibit an employer from requiring an employee to provide log-in information if 'there is specific information about activity on the employee's personal … account', then the provision of information is allowed

> for the purpose of ensuring compliance with applicable laws, regulatory requirements, or prohibitions against work-related employee misconduct … or … [if] the employer has specific information about an unauthorized transfer of the employer's proprietary information, confidential information, or financial data to an employee's personal … account …[40]

So, where the employer has grounds for suspecting that misconduct has taken place, it can compel the employee to hand over log-in information. Leaving aside the question of the reasonableness (or not) of those grounds, the forced disclosure of passwords is a double privacy intrusion — with the handing over of the password arguably being akin to giving the employer the keys to a home — in addition to the information about the employee that may be gained when the password is used.

B *Regulatory Challenges*

The identified tensions pose challenges to the regulation of behaviour in this area. A lens that is useful to apply to the complexity of this issue is that of Black's 'decentred regulation'.[41] Black's idea centres on the way that industries may be regulated where there is no centralised regulatory body. There are, of course, the FWC and the Office of the Australian Information Commissioner

38 The definition of a social media account excludes 'an account provided by an employer or intended to be used primarily on behalf of an employer': 21 V.S.A § 495k(a)(1).

39 Ibid § 485k(b)–(c).

40 Jordan M Blanke, 'The Legislative Response to Employers' Requests for Password Disclosure' (2014) 14 *Journal of High Technology Law* 42, 72, quoting Mich Pub Acts § 478.5 (2012).

41 Julia Black, 'Critical Reflections on Regulation' (2002) 27 *Australian Journal of Legal Philosophy* 1. For an application of this idea to employment contracts, see Chris Dent, 'The (Potential) Regulatory Function of Contractual Clauses: Restraints of Trade and Confidential Information in Employment Contracts' (2013) 26 *Australian Journal of Labour Law* 1. It has also been applied to the regulation of speech generally: Chris Dent, 'Compensation and/or Correcting the Record: A Framework for the Regulation of (Defamatory) Speech' (2011) 16 *Media & Arts Law Review* 123.

('the Commissioner'); however, neither have an explicit responsibility for the regulation of access to employee social media posts.[42] More fully, there are five aspects of the 'decentred understanding' of regulation; these are: 'complexity, fragmentation, interdependencies, ungovernability, and the rejection of a clear distinction between public and private'.[43] It could almost go without saying that this area of regulation is complex and fragmented. The point around the lack of distinction between public and private also seems obvious in the context of social media — though, given the distinction is usually considered in terms of public and private modes of regulation (as opposed to the separation of public and private lives), the point is not quite as obvious as it appears.

A key insight of the theory, for the purposes of this analysis, is that it sees individuals as 'ungovernable' — in the sense that multiple factors impact on any behavioural decision that a particular person makes (in this case, either the employer or the employee). Where there are no laws to limit behaviour, then norms may be a factor that guides the actions of an individual. In the case of accessing a worker's posts, an employer may, in most circumstances, be happy to not look at them — but this may only reflect the norms that the employer chooses to abide by. In some circumstances, however, an employer's usual desire to respect the privacy of the employee may be overridden by a perceived need to investigate an allegation of bad publicity for the company or of illegal behaviour on the part of the employee. An employer's willingness to breach any privacy norm is facilitated by the lack of concrete negative consequences for the breach; that is, there are no sanctions imposed on the employer should they breach a 'mere' norm.[44]

One definition of a norm is the 'common measure' of behaviour within a group.[45] Given that norms are specific to groups, then it is immediately obvious that the norms that relate to employers may not be the same as those that relate to employees. Further, it may be problematic to delineate what such a measure is in a group as diverse as that of Australian employers. One solution to this is, following Nissenbaum, that where online norms cannot be readily identified because the social context in which they apply is novel, as in the case of social media, she suggests that norms governing analogous off-line contexts should prima facie apply.[46] The onus would then be on any party who believed a different norm should apply online to provide compelling policy reasons in support of that view.[47] The issue here is that this suggestion operates only as a presumption and, as a result, does not adequately cover the complexity of the intersecting forms of legal regulation in this area.

42 The specifics of the two modes of centralised regulation will be returned to below.

43 Black, above n 41, 4.

44 There may also be some informal consequences — such as a reputation for being a 'bad boss' (which may not reflect well in the business — but that is not the same as some formal sanction).

45 François Ewald, 'Justice, Equality, Judgement: On "Social Justice"' in Gunther Teubner (ed), *Juridification of Social Spheres: A Comparative Analysis in the Areas of Labor, Corporate, Antitrust and Social Welfare Law* (De Gruyter, 1987) 91, 108 (emphasis altered).

46 Helen Nissenbaum, 'A Contextual Approach to Privacy Online' (2011) 140(4) *Daedalus* 32, 43.

47 Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 *Washington Law Review* 119, 145–6.

One aspect of that complexity relates to the tension between what individuals expect and what the law, in fact, can provide for. A key issue here is the expectation, on the part of the employee, of privacy around social media posts. There is no unanimity here. Some question whether people who disclose personal information on social media should have any expectation of privacy at all. Indeed, in 2010, Mark Zuckerberg, the founder of Facebook, went so far as to say that privacy itself was no longer a 'social norm':

> People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people … That social norm is just something that has evolved over time.[48]

The contrary perspective is offered by other commentators. Clark and Roberts, for example, have expressed concern about the chilling effect that employer surveillance might have on employees , arguing that '[r]ather than expecting users of [these networks] to change their behavior by not posting anything they do not want an employer to view … it is better for society for employers not to enter an employee's virtual front door'.[49] Further, Nissenbaum explicitly rejects the suggestion that information which is publicly accessible cannot be private, arguing that the right to privacy is actually 'a right to live in a world in which our expectations about the flow of personal information', as reflected in societal norms, are generally met.[50] Relating this to the workplace, Nissenbaum has labelled the harvesting of information from social media by employers as prima facie 'morally troubling because it threatens to disrupt the delicate web of relationships that constitute the context of social life'.[51]

Legal expressions around this expectation of privacy are found in the United States: one US court has held, for example, that a person who posted a poem in her public MySpace journal had no reasonable expectation of privacy in its contents, and therefore could not sue a newspaper which had republished the poem for invasion of privacy, even though she had only expected a limited audience and had taken it down within a week.[52] On the other hand, in another decision, it was held that an employee 'may have had a reasonable expectation that her Facebook posting would remain private, considering that she actively took steps to protect her Facebook page from public viewing'.[53] Conversely, in the United Kingdom, it has also been held that a sacked employee did not have a reasonable expectation of privacy in relation to his private posts, such as to engage art 8(1) of the *Convention*

48 Quoted in Bobbie Johnson, 'Privacy No Longer a Social Norm, Says Facebook Founder', *The Guardian* (online), 11 January 2010 <http://www.theguardian.com/technology/2010/jan/11/facebook-privacy>. Admittedly, Zuckerberg's views, at least, may be evolving: see Hayley Tsukayama, 'Is Facebook Learning to Embrace Privacy?', *The Washington Post* (online), 29 July 2014 <https://www.washingtonpost.com/news/the-switch/wp/2014/07/29/is-facebook-learning-to-embrace-privacy/?utm_term=.5a940b2a80a7>.

49 Clark and Roberts, above n 4, 519.

50 Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press, 2010) 231.

51 Ibid 228.

52 *Moreno v Hanford Sentinel Inc*, 91 Cal Rptr 3d 858, 862–3 (Ct App, 2009).

53 *Ehling v Monmouth-Ocean Hospital Service Corp*, 872 F Supp 2d 369, 374 (Martini J) (D NJ, 2012).

for the Protection of Human Rights and Fundamental Freedoms,[54] given that 'the nature of Facebook, and the internet generally, is that comments by one person can very easily be forwarded on to others'.[55]

A further aspect of the 'ungovernability' of employees is that they, to an extent, self-govern. The decision to use passwords to protect access is a clear example of an attempt to limit the audience of posts — with the complexity of the password a function, in part, of the user's balancing of convenience and security. Social media sites, for example, usually also permit users to restrict access to their page to specified individuals. On Facebook, for example, a member may restrict such access to his or her network 'friends' — other members of the site whose request to be a friend has been accepted. In this sense, it is possible to speak of private as opposed to public social media pages.[56] There is evidence that many social networkers already use such settings — 72 per cent of those surveyed by Levin and Abril,[57] a trend that appears to be intensifying over time.[58] This is not a cure-all. Fienberg notes that many problems remain with these settings:

> For example, most users don't realize that when they hide a post or photograph from their … page, that those posts are not truly hidden and can be visible elsewhere, including on another person's page, and are ultimately easily accessible to external third parties.[59]

Further and critically, even if an individual correctly adopts the maximum privacy settings on his or her social media account or chooses not to use social media at all, there is nothing to stop others posting information or images of that person online.[60] Thus, third-party posts can represent significant intrusions on an individual's privacy that are accessible by that individual's employer. To be clear, the third parties who post without permission are outside the scope of most forms of direct regulation. In these circumstances, it is the employer who pays attention to the third-party posts that is the target of regulation.

Two other aspects of decentred regulation will round out this preparatory section. The first is that of interdependency. This aspect highlights the observation that the interests of the employer and the employee are connected — at least with

54 *Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953) art 8(1) provides that '[e]veryone has the right to respect for his private and family life, his home and his correspondence'.

55 *Crisp v Apple Retail (UK) Ltd* (Unreported, Employment Tribunals, Oliver J, 5 August 2011) [44].

56 In fact, this is an oversimplification as, on Facebook at least, certain information such as a member's name will always be publicly available and he or she may choose to make other information public. In these circumstances, the user's profile may be said to have public and private pages. See Facebook Help Centre, *What is Public Information?* (2018) <http://www.facebook.com/help/?faq=167709519956542>.

57 Levin and Abril, above n 17, 1033.

58 Fred Stutzman, Ralph Gross and Alessandro Acquisti, 'Silent Listeners: The Evolution of Privacy and Disclosure on Facebook' (2012) 4(2) *Journal of Privacy and Confidentiality* 7, 7.

59 Stephen E Fienberg, 'Is the Privacy of Network Data an Oxymoron?' (2012) 4(2) *Journal of Privacy and Confidentiality* 1, 1.

60 As Fienberg notes, 'I do not use Facebook, Google+, or any other networking sites and … I do not tweet. I know that I can be found on Facebook and other social networks, but only through postings created by others. Unfortunately, pictures of me and my biographical information are there and I am powerless to remove them': ibid 4.

respect to their financial interests.[61] A company that does well is likely, all other things being equal, to keep an employee employed. This, of course, does not apply where an employee was sacked as a result of a social media post. An associated point is that the interests of both parties are fragmented. Employees, in particular, do not only have financial interests. Their motivations to make problematic social media posts are complex. Thornthwaite notes that social media 'provides new and expanded opportunities' for various forms of employee behaviour including 'mocking management practices, individual managers, and customers, pursuing interests that may conflict with professional obligations, such as theft of intellectual property, and bullying and harassment of colleagues'.[62] This list does not include social interests, or any interests in self-expression. A post made by an employee that criticises their employer could be made so that the employee 'fits in' with a particular group, or it could be a post that the employee thinks is clever or artful.[63] The question then becomes how does the law balance these interests of the employee with the firm's interests (which may be predominantly, but not completely, financial)?

III AUSTRALIAN LAW AND EMPLOYEE-GENERATED SOCIAL MEDIA

This Part of the article will explore the law, as it exists now, and consider the extent to which the system constrains the capacity of employers to monitor the digital expression of their employees.[64] While there is no suggestion that the law is actively seeking to facilitate a return to a nineteenth-century master-servant relationship,[65] there are significant doubts as to the effectiveness of the current settings to appropriately protect the interests of both employer and employee. There are two areas of law that, currently, may impact on an employer's capacity to monitor the personal social media posts of its employees. The first area of law to be discussed here is privacy legislation — though these statutes do not apply to all workplaces. The second is the body of law that has developed around the employment relationship — though again, much of that is aimed at regulating the

61 'Most employees want to do the right thing by their employer — "As an employee, you still have to have your workplace's best interests at heart"': Beatrix M P van Dissel, 'Social Media and the Employee's Right to Privacy in Australia' (2014) 4 *International Data Privacy Law* 222, 232. The quote within the quote is from a qualitative study on the 'current social media behaviour of employees and employers'.

62 Thornthwaite, 'Social Media, Unfair Dismissal and the Regulation of Employees' Conduct Outside Work', above n 24, 167.

63 In *Singh v Aerocare Flight Support Pty Ltd* [2016] FWC 6186 (13 September 2016) [34], the employee claimed that the post that got him sacked was intended to be seen as sarcasm.

64 One form of regulation that will not be considered in detail is the 'anti-hacking' laws, such as div 478 of the *Criminal Code Act 1995* (Cth) sch 1, which makes it an offence for anyone to use a carriage service to cause 'any unauthorised access to … restricted data' held on a computer, including password-protected material, if that person knows the access to be unauthorised. Thepotential breadth of this provision has not been tested, in the employment context, in Australia..

65 Thornthwaite, 'Social Media, Unfair Dismissal and the Regulation of Employees' Conduct Outside Work', above n 24, 165.

behaviour of employees and not the employers. This Part will be rounded out with a critique of the law from the perspective of regulatory theory.

A *Commonwealth Privacy Act*

An Australian employer that wishes to monitor its employees via social media may need to comply with Commonwealth, state or territory privacy legislation regulating the handling of personal information.[66] The focus of discussion will, however, be the *Privacy Act 1988* (Cth), (the '*Privacy Act*').[67] The *Privacy Act* regulates, inter alia, the collection,[68] use and disclosure of 'personal information',[69] being information, including opinion, whether or not recorded in a material form, about an individual, who is identified or reasonably identifiable.[70] The regulation is done through requiring 'APP entities' (being Commonwealth government agencies[71] and some private sector organisations)[72] to comply with its *Australian Privacy Principles* ('*APP*') when dealing with personal information.[73] An entity that fails to do so will be deemed to have interfered with the privacy of the individual concerned.[74] In terms of what may be collected, the *Privacy Act* requires that APP entities may only collect personal information that is 'reasonably necessary' for one or more of its functions or activities,[75] in the sense that it cannot, in practice, effectively pursue the function or activity without collecting the information. By way of clarification, should an employer access, and record, any information from a worker's social media posts, then the employer is likely

66 See, eg, *Information Privacy Act 2009* (Qld).

67 This is because the state and territory legislation is conceptually similar to the Commonwealth legislation but more confined in that it only applies to the respective public sectors of those jurisdictions in which it is found. Further, there is virtually no case law on any of these Acts and, for the purpose of space, it was decided that it was more efficient to go into detail for one statute rather than several.

68 Information is collected for the purposes of the Act if it is collected 'for inclusion in a record or generally available publication': *Privacy Act* s 6(1) (definition of 'collects'). A record includes a 'document' or an 'electronic or other device': at s 6(1) (definition of 'record').

69 *Privacy Act* s 2A.

70 Ibid s 6(1) (definition of 'personal information').

71 This includes government departments and statutory authorities: see ibid s 6(1) (definition of 'agency'). The Act does not apply to state and territory government agencies.

72 Subject to certain exemptions, an organisation is defined as 'an individual; … a body corporate; … a partnership; … any other unincorporated association; or a trust: see ibid s 6C(1).

73 *Privacy Act* sch 1 ('*APP*'). The *APP* replace the *Information Privacy Principles* that applied to agencies and the *National Privacy Principles* that applied to organisations before March 2014.

74 *Privacy Act* s 13(1).

75 *APP* cls 3.1–3.2. The Supreme Court of Victoria has held that the collection of information from an employee's Facebook account for the purposes of a disciplinary investigation was necessary under the equivalent provision, cl 3.1, of the *Information Privacy Act 2000* (Vic): see *Jurecek v Director, Transport Safety Victoria* (2016) 260 IR 327 ('*Jurecek*'). In the case of an agency, the collection of the information is also allowed where it is directly related to one or more of its functions or activities.

to be seen to be 'collecting' information about the employee (for the purposes of the *Privacy Act*).[76]

The *Privacy Act* also requires that entities collect personal information directly from the individual concerned where that is reasonable and practicable.[77] However, in terms of the information on social media which may be of interest to an employer, it would not be practicable to collect much of it directly from a worker, given that they would be unlikely to disclose anything directly to the employer which might prejudice their employment.[78] Further, the *Privacy Act* requires that information be collected by 'fair means';[79] and the Commissioner has suggested it would usually be unfair to collect information covertly.[80] As 'fair means' also must not involve intimidation,[81] it is likely that any forced disclosure of a password would be, prima facie, against the *Privacy Act*. Many, if not most, Facebook and Instagram posts would fit within the definition of 'personal information' and, therefore, their collection should be subject to the *APP* (assuming that the employer is an APP entity).

Moreover, an entity generally cannot collect certain 'sensitive information' about a worker without his or her consent.[82] This includes personal information about the employee's health, racial or ethnic origin, political opinions, membership of a political association or trade union, religious beliefs or affiliations, philosophical beliefs, sexual preferences or practices, or criminal record, as well as genetic information.[83] That said, many employees may feel that in practice they have little choice but to consent to the collection of their sensitive information by their employer,[84] given the underlying inequality of bargaining power that often

76 This is true under the *Privacy Act*, as opposed to some state legislation such as the *Privacy and Data Protection Act 2014* (Vic), even if such posts are considered to form part of a generally available publication. On the question of whether publicly available social media comments do form part of a generally available publication under the Victorian legislation, see *Jurecek* (2016) 260 IR 327, 348–9 [82]–[84].

77 *APP* cl 3.6.

78 Similarly, in *Jurecek* it was held that it would not have been practicable under the equivalent provision of the *Information Privacy Act 2000* (Vic) to collect information directly from the employee rather than her Facebook account where that would have 'undermined the integrity of the disciplinary process': *Jurecek* (2016) 260 IR 327, 361 [154].

79 *APP* cl 3.5.

80 Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines* (31 March 2015) [3.62] <http://web.archive.org/web/20180114022007/https://www.oaic.gov.au/resources/agencies-and-organisations/app-guidelines/APP_guidelines_complete_version_1_April_2015.pdf>. See also Office of the Federal Privacy Commissioner, *Guidelines on Workplace Email, Web Browsing and Privacy* (30 March 2000) <https://web.archive.org/web/20090709042040/http://www.privacy.gov.au/internet/email/>; *Griffiths v Rose* (2011) 192 FCR 130, 141 [26].

81 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 77.

82 *APP* cl 3.3. Although a 'clear connection' must exist for information to be 'directly related to' an agency's functions or activities, this alternative test may mean that agencies have to meet 'a slightly lower threshold' for collection of information than do organisations: see Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 75.

83 *Privacy Act* s 6(1) (definition of 'sensitive information').

84 Consent under the Act may also be implied, suggesting that an employee who continued in his or her employment without complaint after having received notice that such information might be collected from social media, may also be held to have consented to its collection: see *Privacy Act* s 6(1) (definition of 'consent').

characterises the employment relationship.[85] Absent consent, an entity may also collect sensitive information where it 'has reason to suspect … unlawful activity, or [serious] misconduct', including breach of duty, 'that relates to its functions or activities … [and it] is necessary [to collect the information] in order to take appropriate action in relation to the matter'.[86] Information gleaned from 'social discovery' sites, such as Grindr, is likely to fall within the category of 'sensitive information' but is not likely to be connected to an investigation into 'unlawful activity' or 'serious misconduct'.

Importantly, under the *Privacy Act*, '[a]n APP entity must have a clearly expressed and up-to-date policy … about [its] management of personal information',[87] which must include information about 'the kinds of personal information [it] collects and holds', how it collects and holds that information; and for what purposes.[88] It must also take reasonable steps to make that policy available free of charge and in an appropriate form.[89] An entity is also required to notify or make an individual whose personal information it collects aware of what kind of information is being collected and why.[90] If practicable, it must do so at or before the time of collection. The *Privacy Act* also provides that if the information is being collected from someone other than the individual concerned, he or she should be informed of the circumstances of collection,[91] which may include the method of collection.[92] These processes make the management of information more transparent; however, in the employment context, they may not compensate for the imbalance of power between the employer and the employee.

Finally, where an employee believes his or her employer has interfered with their privacy by breaching an *APP*, he or she can lodge a complaint with the Commissioner.[93] If the complaint is found to be substantiated, the Commissioner may make a determination declaring that the respondent should not repeat or continue the behaviour which has interfered with the complainant's privacy.[94] The Commissioner may also declare that the complainant is entitled to compensation,

85 As the VLRC has noted, '[i]ndividual workers often have little real power to object to practices that affect their privacy. They may be required to agree to such practices to obtain or keep a job': VLRC, above n 7, 23 [2.23]. While this raises a question as to whether such consent can be considered genuine consent for the purposes of the Act, Australian courts have generally been reluctant to recognise the element of implicit coercion that may exist in the employment relationship: see Julian Sempill, 'Under the Lens: Electronic Workplace Surveillance' (2001) 14 *Australian Journal of Labour Law* 1.

86 *APP* cl 3.4(b); *Privacy Act* s 16A item 2.

87 *APP* cl 1.3.

88 Ibid cl 1.4.

89 Ibid cl 1.5.

90 Ibid cl 5.1; *The Tenants' Union of Queensland Inc and TICA Default Tenancy Control Pty Ltd* (Unreported, Federal Privacy Commissioner Complaint Determination No 4 of 2004, Commissioner Crompton, 16 April 2004) 15 [76].

91 *APP* cls 5.1(a), 5.2(b).

92 Office of the Australian Information Commissioner, above n 80, [5.11].

93 *Privacy Act* s 36. The Commissioner, who has assumed the statutory powers of the Federal Privacy Commissioner under the Act, can also investigate possible breaches of the Act on his own initiative: see s 40(2).

94 *Privacy Act* s 52.

including for injury to feelings or humiliation suffered.[95] If an individual is found to have lost his or her job as a result of their employer's breach of the *Privacy Act*, the amount of damages awarded could potentially be substantial. In a case involving serious or repeated breaches of an individual's privacy, the Commissioner may also accept an enforceable undertaking,[96] or apply to the court for the imposition of a civil penalty of up to $2.1 million for a body corporate or $420 000 for individuals.[97]

The *Privacy Act* might then be thought to at least go some way towards addressing privacy concerns raised by employer access to personal employee social media. However, although the Australian Law Reform Commission ('ALRC') has called for their removal,[98] the Act remains subject to two important exceptions which significantly reduce its application to private sector employees. First, small businesses, being businesses with an annual turnover of $3 million or less, are currently generally exempt from the Act.[99] This means that most private sector employers are simply not subject to its provisions.[100] Secondly, the acts or practices of an organisation that directly relate to an individual's employment and their 'employee record', being 'a record of personal information relating to the employment of the employee',[101] which can include information about, inter alia, the employee's health, performance or conduct,[102] are also exempt from the Act.[103]

This exemption would allow a private sector employer who is subject to the Act to freely collect even sensitive information about an employee from social media, if this action directly relates to their employment. While the precise scope of

95 Ibid ss 52(1)(b)(iii), 52(1AB). However, if an organisation did not comply with the Commissioner's declaration, it would be necessary to commence enforcement proceedings in either the Federal Court or Federal Circuit Court, which would re-hear the complaint: see *Privacy Act* s 55A.

96 Ibid s 33E.

97 Ibid ss 13G, 80W(5).

98 ALRC, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) vol 2, 1358 (Recommendation 39–1), 1397 (Recommendation 40–1).

99 *Privacy Act* ss 6C(1), 6D. However, this exemption is subject to certain exceptions set out at s 6D(4).

100 In 2000, it was estimated that approximately 94 per cent of Australian businesses fell within this exception: see Commonwealth, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000*, Parl Paper No 130 (2000) 11 [2.20].

101 *Privacy Act* s 6(1) (definition of 'employee record').

102 Ibid. Amongst other things, an employee record can also include information about the disciplining or termination of employment of the employee.

103 Ibid ss 7(1)(ee), 7B(3). For a discussion of the provisions, see Amanda Pyman, Anne O'Rourke and Julian Teicher, 'Information Privacy and Employee Records in Australia: Which Way Forward?' (2008) 34 *Australian Bulletin of Labour* 28.

this exception is unclear,[104] it appears to be intended to operate broadly.[105] It will presumably allow an employer to collect posts made after hours, or which relate to an employee's behaviour outside of work, if the post also breaches or evidences a breach of the employment contract. If so, it will allow the employer to collect posts which call into question the employee's fitness to perform their duties,[106] or are 'capable of harming the reputation or efficient management of the employer's business',[107] or which evidence behaviour of this nature. Arguably the exemption might even allow an employer to collect any posts which, though not fitting this description, refer to the employer, co-workers, or incidents at work. These possibilities suggest that the employee records exemption allows employers to intrude on an employee's private life to an extent that many workers would be unhappy with.

B *Workplace Regulation*

There are three aspects of the law of the workplace that are relevant here. They are the blunt-force tool of dismissal of the employee and the ways in which that action may be found to be unfair, the relevance of an employer's policies, and the new 'anti-bullying' provisions of the *Fair Work Act 2009* (Cth) (*'Fair Work Act'*). By way of context, given the relative lack of explicit privacy protection in Australia, there has been less discussion of the expectation of privacy in the context of social media when compared to the US and UK examples referred to above. One characterisation, however, is evident in *Linfox Australia Pty Ltd v Stutsel*,[108] a case in which an employee successfully challenged his dismissal on the basis of comments on his Facebook page. On appeal, it was held that:

> The fact that the conversations were conducted in electronic form and on Facebook gave the comments a different characteristic and a potentially wider circulation than a pub discussion. Even if the comments were only accessible by the 170 Facebook 'friends' of the Applicant, this was a wide audience and one which included employees of the Company. Further the nature of Facebook (and other such electronic communication on the internet) means that the comments might easily be forwarded on to others, widening the audience for their publication. Unlike conversations in a pub or cafe, the Facebook conversations leave a

104 The few cases dealing with the scope of this exemption provide little guidance in this context. For conflicting views on the operation of the exemption in relation to employee e-mail or web browsing history, see 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, Hiroya Nakakubo and Takashi Araki (eds), *Protection of Employees' Personal Information and Privacy* (Wolters Kluwer, 2014) 7, 23–4.

105 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth) states at page 5 that: 'An employee record is defined broadly … and includes the types of records typically held by employers on personnel files'. It adds that the requirement that the act or practice must be directly related to an employment relationship is designed 'to ensure that employers cannot use employee records for commercial purposes unrelated to the employment context'.

106 The exemption will not apply in favour of a third party such as a private investigator or a social media monitoring agency engaged by the employer, at least in the absence of an agency relationship.

107 Andrew Stewart, *Stewart's Guide to Employment Law* (Federation Press, 5th ed, 2015) 262.

108 (2012) 217 IR 52.

> permanent written record of statements and comments made by the participants, which can be read at any time into the future until they are taken down by the page owner.[109]

This suggests that there should be no expectation of privacy — as, no matter what practices the original poster adopts, they have little control over the actions of others.

1 *Background Issues*

Given the contractual relationship between the employer and the employee, the relationship can come to an end. An employer may, therefore, dismiss an employee based on the employer's reaction to a social media post of the employee. This may have a prejudicial impact on the employee and so the *Fair Work Act* places limits on the employer's capacity to sack people — classifying certain dismissals as 'unfair' and others may be found to be 'unlawful terminations'. Generally speaking, under Australian law even behaviour outside of working hours can amount to a breach of an employment contract if it has a sufficient connection to work because, for example, it affects 'the reputation, success or efficient operation' of the business or organisation.[110] In this regard, there have been a number of unfair dismissal cases involving social media posts that have upheld the dismissal of employees based on their social media comments, even when the posts were made on private pages outside of work time, if those comments could cause serious harm to the business.[111]

The *Fair Work Act* states that where a 'dismissal was harsh, unjust or unreasonable', then the dismissal may be 'unfair'.[112] The first criterion to be used by the FWC when assessing the nature of the dismissal is 'whether there was a valid reason for the dismissal related to the person's capacity or conduct (including its effect on the safety and welfare of other employees)'.[113] Of course, not all conduct, and not even all offensive conduct, will justify a dismissal. One employee, for example, who posted a video of 'sexually explicit nature' on Facebook and tagged a couple of colleagues successfully fought his dismissal on the grounds that it was unfair.[114]

The *Fair Work Act* also prohibits an employer taking adverse action against an employee on various grounds including 'race, … sexual orientation, age, physical or mental disability, marital status, family or carer's responsibilities, pregnancy,

109 Ibid 61 [26]. Compare the comments of the UK's Trades Union Council: employers 'wouldn't follow an employee down the pub to check on what they said to their friends about their day at work. Just because they can do something like this online, doesn't mean they should': Andrea Broughton et al, 'Workplaces and Social Networking: The Implications for Employment Relations' (Research Paper No 11/11, Advisory, Conciliation and Arbitration Service, 2010) 22.

110 Andrew Stewart et al, *Creighton & Stewart's Labour Law* (Federation Press, 6th ed, 2016) 499.

111 See Forsyth, above n 104, 28–9. His analysis shows that an employer's failure to have an enforceable policy in place governing its employees' use of social media has been an important factor in some dismissals being held to be unfair.

112 *Fair Work Act* s 385.

113 Ibid s 387(a). The other criteria include a number relating to procedural fairness and the catch-all criterion of 'any other matters that the FWC considers relevant': at s 387(h).

114 *Renton v Bendigo Health Care Group* [2016] FWC 9089 (30 December 2016).

religion, political opinion, national extraction or social origin'.[115] Therefore, an employee who has been dismissed could allege that the employer's actions were in reality motivated by one of these prohibited grounds of which it had become aware through monitoring of his or her social media (for example, where a homophobic employer is made aware of an employee's Grindr profile). If that individual is able to show a prima facie case of discrimination, then the employer would bear the onus of proving that the employee was not dismissed for a prohibited reason or for reasons that included that reason.[116] Whilst there are many more social media cases fought under the unfair dismissal provisions, one example of an unlawful termination case is *McIntyre v Special Broadcasting Services Corporation* — where the employee posted 'social media comments … on Anzac Day regarding, inter alia, Australian Defence Force personnel engaged in various theatres of war'.[117]

It is also possible, but highly unlikely under the current system, that an *employer* could be held to have breached a duty to the employee when the employer acts against that employee. There are two possible duties that are relevant here — a duty of mutual trust and confidence and a duty of good faith. With respect to the former, in the UK at least, an employer is bound by an implied contractual duty to not, without reasonable cause, conduct itself in a manner likely to seriously damage the relationship of trust and confidence between itself and its employees.[118] Such a duty might prevent, at least, covert surveillance of employees.[119] However, the High Court has recently held that no such duty is implied by law into Australian contracts of employment. Nor was such a duty implied by fact into the contract of employment before the Court.[120] Pittard and Naughton's analysis of the High Court's decision suggests that it 'leaves open the question whether it might be "necessary" to imply such a term in other contracts of employment'.[121] Further, an implied duty of good faith that binds the employer has not been explicitly excluded from Australian law.[122] As Riley has argued, such a duty could and should be introduced via statute as the courts have been very reluctant to find it within the body of the case law.[123] It is not clear, however, whether any implied duty of good faith, or of mutual trust and confidence, would prevent an employer accessing social media posts that are already publicly accessible.[124] It would be

115 *Fair Work Act* s 772.

116 Ibid s 385. See also s 783.

117 [2015] FWC 6768 (1 October 2015) [7].

118 *Malik v Bank of Credit and Commerce International SA (in liq)* [1998] AC 20.

119 Stewart et al, above n 110, 712–13 [21.42].

120 *Commonwealth Bank of Australia v Barker* (2014) 253 CLR 169 ('*Barker*').

121 Marilyn J Pittard and Richard B Naughton, *Australian Labour and Employment Law* (LexisNexis Butterworths, 2015) 296.

122 As noted by Kiefel J in *Barker* (2014) 253 CLR 169, 214 [107].

123 Joellen Riley, 'Before the High Court: "Mutual Trust and Confidence" on Trial: At Last' (2014) 36 *Sydney Law Review* 151, 166.

124 Other commentary is clearer — 'nor is there any authority extending an employer's implied duties to cover employee privacy': Carolyn Sappideen et al, *Macken's Law of Employment* (Lawbook, 8th ed, 2016) 197.

less controversial to suggest that either duty would limit the capacity for the employer to act surreptitiously when accessing any posts.

2 *Role of Workplace Policies*

A key form of conduct that may give rise to a dismissal is the breach of a workplace policy.[125] The concern here is that the policies tend to bind the employee and not the employer. A company may, for example, have a social media policy that limits what a worker may say online, but that says little about the behaviour of the boss. Where a company does have a social media policy, then the employer may feel entitled to track the social media posts of its employees in order to see if the policy is being complied with. Such a policy may have a 'chilling effect' on the employee on the basis that most employees will not have an accurate idea as to how enforceable a particular policy is.

For an employer to lawfully dismiss an employee for a failure to comply with a policy, the policy, and its communication, have to comply with a number of legal requirements. In short, however, '[a] failure to comply with a lawful and reasonable policy is a breach of the fundamental term of the contract of employment that obliges employees to comply with the lawful and reasonable directions of the employer'.[126] A policy may be incorporated into the contract of employment as either an express or an implied term of the contract,[127] but it does not have to be.[128] That is, a policy may have some relevance, even if it is not incorporated into the contract, in the determination of 'whether the employer breached the implied term of mutual trust and confidence'[129] should such a term be implied into the contract. Second, the courts have said that employers may 'not act capriciously' and 'arguably [can]not act unfairly' towards employees when it comes to applying policies.[130] Further, the enforceability of the policies

125 For a study into the social media policies of Australian firms, see Thornthwaite, 'Chilling Times', above n 35. For a general discussion of the law and social media policies, see Pauline Rapaport, 'Social Media Policies and Unfair Dismissal' (2013) 18 *Media & Arts Law Review* 75.

126 *B v Australian Postal Corp* (2013) 238 IR 1, 15 [36].

127 See, eg, the discussion in *Commonwealth Bank of Australia v Barker* (2013) 214 FCR 450; revd *Barker* (2014) 253 CLR 169. The case in the Federal Court of Australia involved the policy operating as an implied term to the contract. The case in the High Court of Australia did not revisit the question of a workplace policy operating as an implied term.

128 This is '[t]he most straightforward way of ensuring that work rules have contractual force': Stewart et al, above n 110, 282 [11.12].

129 Craig Cameron, 'Policies That Don't Bind: The Decision in *Akmeemana v Murray*' (2010) 23 *Australian Journal of Labour Law* 137, 140.

130 *Riverwood v McCormick* (2000) 177 ALR 193, 223 [152] — though the sentiment, strictly speaking, was about amending the policies.

may depend on the extent to which the employee has been made aware of,[131] or received training in, those policies.[132] Finally, there is the question of whether 'a reasonable person would believe' that a particular policy statement would 'form part of an enforceable contract'[133] — as has been noted, 'in the absence of express agreement of the parties, the enforceability or otherwise of such policies will depend on the particular circumstances of each case'.[134] This means that the employee, already in a position of less power than the employer, may not have a clear idea of the legal status of the social media policy (which is not a good outcome from a regulatory perspective).

Where there is a question mark over the validity of a policy, it may be that in practice the only recourse to actions taken on the basis of that policy is for an employee to sue for unfair dismissal when a breach of the policy resulted in the employee losing her or his job. That is, as social media policies tend to bind the employee (they are not 'promissory words' from the employer),[135] any sanctions are aimed at the employee. So, the manifestation of an employer doing the wrong thing with respect to a policy is the employer sacking the employee. The recourse for such 'bad behaviour' is for the ex-employee to sue the employer. If, however, the employer does not sack the employee for breaching the policy, then there is no sanction for the employer checking the employee's social media posts. Even if the employee is dismissed, the sanction relies on the worker having the resources, and willingness, to bring an action against the employer. It may be best said, then, that the currently available modes of soft regulation do not place any significant restrictions on employers with significant motivations to monitor a worker's social media communications.

131 Giancaspro, in his 'advice' for employers, notes that

> [i]t is critical that a thoroughly drafted policy is effectively implemented in the workplace and there are a number of ways to accomplish this. The policy should be widely disseminated throughout the workplace and made readily available to employees to ensure there are no concerns as to access or knowledge of its existence. … Training should occur regularly and take account of recent changes to policies and legislation where applicable.

Mark Giancaspro, 'Do Workplace Policies Form Part of Employment Contracts? A Working Guide and Advice for Employers' (2016) 44 *Australian Business Law Review* 106, 117.

132 See, eg, *Pearson v Linfox Australia Pty Ltd* [2014] FWCFB 1870 (17 January 2013). This case focuses on the social media policy of the employer, and the fact that the employee received one-on-one training about the policy.

133 Rosemary Owens, Joellen Riley and Jill Murray, *The Law of Work* (Oxford University Press, 2nd ed, 2011) 252 [6.3.4.1].

134 Pittard and Naughton, above n 121, 57 [2.18].

135 With respect to policies as promissory words, see *Goldman Sachs JBWere Services Pty Ltd v Nikolich* (2007) 163 FCR 62. For a discussion of that case, see Louise Keats, 'Workplace Policy as Contract: The Full Federal Court Hands Down Its Decision in the *Nikolich* Appeal' (2008) 21 *Australian Journal of Labour Law* 43.

3 *Anti-Bullying Provisions*

There is one other, potential, sanction in the *Fair Work Act.* This sanction relates to the 'bullying' provisions in the Act.[136] With respect to the FWC's powers in the area, its 'jurisdiction … is intended to be preventative, to resolve the issues and to restore working relationships, and not to make financial compensation or to penalise employers'.[137] Importantly, a successful action under the Act requires that there be repeated bullying behaviour rather than a single instance.[138] Two further aspects need to be referred to. First, a 'reasonable management action' will not constitute bullying.[139] Second, given the lack of state referral legislation in this area,[140] the provisions only relate to constitutional corporations, the Commonwealth, Commonwealth authorities, bodies incorporated in a territory, or where the 'business or undertaking is conducted principally in a Territory or Commonwealth place'.[141] This means that many employers would not be bound by the provisions. Without the co-ordinated actions of the states and territories to regulate other businesses, there is a real risk that inequalities will persist in the system. As not all businesses are covered by the Act, or the *Privacy Act*, some employees may have their social media better protected than other employees — not an equitable outcome.

Applying these provisions to employer access to employee social media, on the surface, it is at least arguable that pressuring an employee into divulging a password may create a risk to the psychological health of the employee.[142] However, a single demand, that is acquiesced to, will not meet the hurdle of repeated behaviour. It is also possible though that any ongoing surveillance of social media posts could be seen as problematic under these provisions. As long as the employee can demonstrate that the behaviour of the employer was unreasonable and that it created a risk of psychological harm to the employee,[143] then the action may succeed. Ongoing surveillance may be seen to meet the 'repeated' test in the Act.[144]

136 *Fair Work Act* ss 789FF–789FG. For a discussion of bullying via social media — rather than an employer bullying an employee into giving access to posts, see *Bowker v DP World Melbourne Ltd* (2014) 246 IR 138.

137 Stewart et al, above n 110, 704 [21.27]. The authors note that, as of 'the end of 2015, only six orders had been made by the FWC, the first five with the consent of the parties': at 705 [21.29].

138 *Fair Work Act* s 789FD(1)(a). In *Re Sun*, an instance of an employee being asked to do work that he did not feel qualified to do was not considered to be bullying behaviour: *Re Sun* (2014) 244 IR 145.

139 *Re SB* (2014) 244 IR 127, 130 [11].

140 Pittard and Naughton, above n 121, 580.

141 *Fair Work Act* s 789FD(3). See also *Re SW* [2014] FWC 3288 (2 June 2014).

142 *Fair Work Act* s 789FD(1)(b).

143 Ibid s 789FD(1). The provision only refers to the 'health and safety' of workers; however, psychological health may be covered too. 'Health', for the purposes of the *Work Health and Safety Act 2011* (Cth) is defined to include 'psychological health': at s 4 (definition of 'health').

144 *Fair Work Act* s 789FD(1)(a).

C *Current Law from a Regulatory Perspective*

The application of the theory of decentred regulation appears to be a good fit for understanding the issue of employer monitoring of personal employee social media posts. For a start, the regulation is fragmented across both workplace and privacy law; and the range of relevant provisions in each area of law reinforces the notion of complexity. In terms of the blurring of the distinction between public and private, the employers are regulated by the law and, in turn, regulate the behaviour of employees. Further, policies (evident in both privacy and workplace law), which are a private tool of regulation created by employers, may be given (public) legal effect. Those characterisations are simply descriptive. The value of this approach is evident in the discussion that becomes available through the use of this perspective.

The final two aspects of the theory apply to employers, employees and the relationship between both categories. Both employers and employees may be seen as 'ungovernable'.[145] As a reminder, this means that both groups should be understood in terms of having multiple factors impacting on any behavioural decision that they make. The two legal regimes facilitate their ungovernability in this area because the laws are not based on clear sanctionable limits to their behaviour. The tests in the *Privacy Act* privilege 'reasonableness'[146] and in the *Fair Work Act*, reasons only have to be 'valid' for a dismissal[147] and the enforceability of policies 'depend[s] on the particular circumstances of each case'.[148] The contingent nature of the law is not, in and of itself, a concern; however, it does mean that the regulated parties must look to norms, amongst other things, to guide their actions.

The differing motivations experienced by the two sides also impact.[149] Both employers and employees have their own interests to protect — though, to an extent, their financial interests are interdependent. The current law does offer a tool to balance these interests.[150] It would be possible for the application of the *Privacy Act* to import a 'proportionality' test into this area of regulation. The Act requires that information be collected by 'fair means';[151] and the Explanatory

145 There are also, in the regulatory mix, the social media connections of the employee who may tag a post and, thereby, make it more public than it was ever intended to be. The final category is outside any regulatory scheme that is either in place or proposed — and, therefore, fully 'ungovernable' in this space and outside this analysis.

146 See, for example, *APP* cls 3.1–3.2 and their reference to 'reasonably necessary'.

147 *Fair Work Act* s 387(a).

148 Pittard and Naughton, above n 121, 57.

149 For two explorations of how the motivators of parties intersect with the law, albeit in other areas, see Chris Dent, 'Decisions around Innovation and the Motivators That Contribute to Them: Patents, Copyright, Trade Marks and Know-How' (2016) 6 *Queen Mary Journal of Intellectual Property* 435; Chris Dent, 'Unpacking Post-Employment Restraint of Trade Decisions: The Motivators of the Key Players' (2014) 26(1) *Bond Law Review* 1.

150 Though it may be that the law, in the practice of workplace law, privileges the interests of one over the other. Sappideen et al note the 'willingness by courts to protect an employer's reputational interests based on assumed harm to its brand even in relation to an employee's conduct or communications outside the workplace', above n 124, 199 [5.405].

151 *APP* cl 3.5.

Memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) states that a fair means of collection is one that is, inter alia, not 'unreasonably intrusive'.[152] While neither the Act, nor the explanatory memorandum, explain the meaning of this phrase, arguably it could also mean that the Act requires an entity to show that any collection of its employees' personal information from social media satisfies a test of proportionality. Certainly, the explanatory memorandum states that '[i]n order for an interference with the right to privacy to be permissible, the interference must be … for a legitimate objective and … necessary and proportionate to that objective'.[153] To comply with such a test, an employer would have to show, inter alia, that any collection of its employees' personal information from social media was the minimum necessary for achieving a legitimate aim and justified in the sense that the societal benefits of the collection outweigh any adverse privacy effect.[154] Currently, however, it appears that the Commissioner does not interpret the Act as imposing a requirement of proportionality on an entity's collection of personal information,[155] or more generally, given that there is no mention of the concept in the *Australian Privacy Principles Guidelines* issued by his office.[156]

The flexibility of an assessment of interests may be attractive, particularly when the legal regime has to encompass significant differences across the range of industries across Australia and the diversity in employees.[157] Expressed differently, the range of parties and their capacities means that regulating this area of activity is difficult. Note how this is a different articulation to the tests described in the *Fair Work Act* and the *Privacy Act*. A question focused on the guiding of behaviour is categorically different to a post facto assessment of whether a specific action was either reasonable or proportionate.[158] Legal tests

152 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 77.

153 Ibid 46.

154 The classic proportionality test also requires that the interference be effective in the sense that it is capable of achieving its desired objective: see Janneke Gerards, 'How to Improve the Necessity Test of the European Court of Human Rights' (2013) 11 *International Journal of Constitutional Law* 466, 469.

155 That said, in an interpretation of the *Information Privacy Act 2000* (Vic), the test of 'reasonable proportionality' was introduced into a decision around an employer's access to an employee's Facebook page: *Jurecek* (2016) 260 IR 327, 346 [70]. This use of the test here was supported by the relevance of the *Charter of Human Rights and Responsibilities Act 2006* (Vic) and the *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) that informs the Victorian *Charter*.

156 Nor do the Guidelines explain when collecting information might be considered unreasonably intrusive. However, earlier guidelines suggest this phrase may be interpreted narrowly: see Office of the Federal Privacy Commissioner, 'Plain English Guidelines to Information Privacy Principles 1 – 3' (Guidelines, October 1994) 6, 26 <https://www.oaic.gov.au/privacy-law/privacy-archive/privacy-guidelines-archive/guidelines-to-information-privacy-principles-1-3>.

157 It should also be noted that the analysis applies to anonymous posts as well as those with a known author. The interest of the employer does not change in relation to the identification of the poster; nor do those of the employee, save for the interest in anonymity. An anonymous poster may feel that they can say more if they think that they are unidentifiable; however, it is not clear that their interest in self-expression changes as a result of those circumstances.

158 The underlying definition of regulation used here is the 'intentional activity of attempting to control, order or influence the behaviour of others': Christine Parker et al, 'Introduction' in Christine Parker et al (eds), *Regulating Law* (Oxford University Press, 2004) 1, 1, quoting Black, above n 41, 25.

are aimed at settling specific disputes; whereas regulation, more generally, may be aimed at preventing disputes arising. Seeking to better regulate the actions of employers, and employees, requires a wider perspective. This is where norms can be developed — though there are added difficulties there, given the range of occupations and professions in the modern economy. The state, of course, has a role in setting minimum standards that would underpin the norms.[159] It is arguable that the *Fair Work Act* and the *Privacy Act* operate in such a manner. The concern here is that the limited application of the statutes means that they are the exception not the rule; this limits their capacity to support universally accepted norms.

Finally, employees may be seen as ungovernable, but total freedom of action is not a result of that characterisation. Employees have fewer resources, and less power in the relationship,[160] than their employers. Despite this imbalance, employees have to take action themselves when they perceive there to be an issue. Even going to the Commissioner with a complaint would, potentially, have a significant impact on the relationship between the employer and the employee; as such, this remedial process does not take account of the contextualised nature of the employee's position.[161] With respect to workplace law, the above discussion highlights that, in most cases, the *Fair Work Act* can provide a remedy for improper access to social media posts — but only where the employee has been sacked.[162] This, obviously, limits the capacity for the employee to act in such a way as to protect their interests. If an employee's privacy is considered worthy of protection, then that protection should be available for all breaches, rather than just those that end up with the employee's termination.

IV PROPOSED REFORMS

This Part will conclude with a discussion of two specific reforms that have been proposed. The first, a statutory tort of privacy, is aimed at better protecting privacy generally. The second, a Recommendation of the VLRC, is for a workplace privacy regulator — an option more specifically targeted at the behaviour of those

159 In the same way that the rules about the maximum blood alcohol concentration underpin the norms around not drinking and driving.

160 The power of employers in this area includes the setting of policies and a degree of choice around the personal information that they collect. It may be noted, however, that collection of personal information in the employee record — while being an acknowledgement of the employer's interest in information — is a matter of practical, rather than theoretical, importance.

161 The argument here is not that it should — as the system is in place for all privacy complaints, rather than just those arising in the workplace — the point here is only to highlight this limit of the process.

162 As another example of such a successful action, see *Smith v Fitzgerald [No 2]* (2011) 204 IR 305.

in the workplace.[163] As with the previous Part, there will be an analysis, at the end, that critiques the two reforms from a regulatory perspective.

A *Tort of Privacy*

By way of background, in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*,[164] the High Court left open the possibility that Australian law might come to recognise a tort of privacy. However, in the almost two decadessince that decision, only two inferior courts have held a privacy tort to exist,[165] while the Supreme Court of South Australia held in 2013 that Australian law is yet to recognise such a tort.[166] Further, in *Giller v Procopets*,[167] the Victorian Court of Appeal awarded damages for a breach of confidence over a videotape of sexual activity involving the plaintiff — with the Court declining to accept the existence of a tort of privacy. Neave J stated that the High Court's approach in *Australian Broadcasting Corporation v Lenah Games Meats* — 'of strengthening the protection afforded to privacy interests by existing causes of action — supports my conclusion that damages should be available for breach of confidence occasioning distress'.[168]

That said, having previously called for the introduction of a statutory cause of action to protect privacy,[169] the ALRC recommended in 2014 that this take the form of a statutory tort.[170] Under the Commission's proposal, the action would be available for serious invasions of privacy by intrusion upon an individual's seclusion or private affairs or misuse of their private information where, inter alia,

163 It may also be noted that the VLRC recommended the introduction of a Workplace Privacy Bill, a recommendation supported by others: see, eg, Witzleb, above n 7, 146. Beyond the Recommendation to be discussed below, one other concern may be raised. The regulatory impact of the title of any such Bill needs to be considered — that is, any attempt to regulate the behaviour of an individual will be facilitated by the greater clarity of the regulatory message. Expressed differently, '[f]rom a regulatory perspective, the clearer the definition of the required standard … the easier is the communication of those standards. The more effective the communication of the required norms, the higher is the level of compliance with the regulation concerned': Chris Dent, 'Copyright as (Decentred) Regulation: Digital Piracy as a Case Study' (2009) 35 *Monash University Law Review* 348, 375. If the purpose of the legislation was to restrict access to a worker's social media posts, then much of the potentially accessible material will be posted from outside the place of employment. It may do a disservice to the regulatory value of the Bill to call it a 'Workplace Privacy Bill' — it may be better to include any such regulation in a broader piece of legislation aimed at protecting privacy more generally.

164 (2001) 208 CLR 199.

165 *Grosse v Purvis* [2003] Aust Torts Reports ¶81-706; *Doe v Australian Broadcasting Corporation* [2007] VCC 281 (3 April 2007).

166 *Sands v South Australia* [2013] SASC 44 (5 April 2013).

167 (2008) 24 VR 1.

168 Ibid 102 [431]. As an aside, Justice Neave was the Chairperson of the VLRC when its Report into Workplace Privacy was released: VLRC, above n 7.

169 ALRC, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) vol 3, 2535 [74.1], 2584 (Recommendation 74–1).

170 ALRC, *Serious Invasions of Privacy in the Digital Era*, Report No 123 (2014) 59 (Recommendation 4–1), 69.

that individual had a reasonable expectation of privacy[171] and the invasion was intentional or reckless. One final element is that 'for the plaintiff to have a cause of action, the court must be satisfied that the public interest in privacy outweighs any countervailing public interest'.[172] Notably, the elements of the proposed tort, insofar as an intrusion is alleged, largely reflect those in the US tort of intrusion upon seclusion.[173]

The immediate difficulty for a worker who sought to object to an employer monitoring his or her personal life via public social media pages would be to establish a reasonable expectation of privacy, given that the pages would be publicly accessible.[174] This approach reflects the broad US position that an individual can have no expectation of privacy in what he or she knowingly exposes to the public.[175] It leaves little room for any expectation of privacy or seclusion in a public social media page where an individual does not attempt to conceal their affairs.[176] A similar approach could be taken by an Australian court in considering the scope of a statutory tort of privacy, given that the ALRC has suggested that a person who may be said to have '[invited] publicity cannot expect the same level of privacy' as someone who has manifested a desire not to have their privacy invaded.[177]

Where private information has been posted online by a third party without consent, rather than by the employee, the worker may be able to argue that any

171 The ALRC recommended:

> in determining whether a person … would have had a reasonable expectation of privacy … the court may consider, among other things: (a) the nature of the private information … (b) the means used to obtain the private information or to intrude upon seclusion … (c) the place where the intrusion occurred … (d) the purpose of the misuse, disclosure or intrusion … (e) how the private information was held or communicated … (f) whether and to what extent the private information was already in the public domain; (g) the relevant attributes of the plaintiff, including … age, occupation and cultural background; and (h) the conduct of the plaintiff, including whether the plaintiff invited publicity or manifested a desire for privacy.

Ibid 96 (Recommendation 6–2).

172 Ibid 144 (Recommendation 9–1).

173 Most US jurisdictions recognise four privacy related torts including intrusion upon seclusion and public disclosure of private facts: see *Restatement (Second) of Torts* (1977) §§ 652B, 652D.

174 If the breach of confidence action was expanded, a similar problem would occur. An individual who sought to argue that some publicly accessible material on their social media site was confidential would have to show, inter alia, that it was not in the public domain. As disclosure to a small group of people does not necessarily put information in the public domain, particularly if the recipients understood that it was to remain confidential, it could perhaps be argued that this material was not in the public domain if only a small number of friends had actually visited the site. However, such Australian authority as there is on the point has held that 'everything which is accessible through resort to the internet … [is] in the public domain': *EPP v Levy* [2001] NSWSC 482 (6 June 2001) [20] (Barrett J), cited in *Australian Football League v The Age Co Ltd* (2006) 15 VR 419, 432 [54].

175 *Katz v United States*, 389 US 347 (1967).

176 Adam Pabarcus, 'Are "Private" Spaces on Social Networking Websites Truly Private? The Extension of Intrusion Upon Seclusion' (2011) 38 *William Mitchell Law Review* 397, 409.

177 ALRC, *Serious Invasions of Privacy in the Digital Era*, above n 170, 105 [6.75]. In the UK, it has been held that the author of an anonymous, publicly accessible blog had no reasonable expectation of privacy in his identity for the purposes of its common law tort of misuse of private information because 'blogging is essentially a public rather than a private activity': *Author of a Blog v Times Newspapers Ltd* [2009] EWHC 1358 (QB) [11], [33].

unauthorised collection or use of that information by their employer would be a prima facie misuse of private information. In this regard, the ALRC has also suggested both that information should not automatically cease to be private once it is in the public domain, and that this type of invasion of privacy should not be confined to unauthorised disclosure, as the collection or other use of private information may also invade a person's privacy.[178] Even if this argument were accepted though, it may not apply to much potentially damaging content posted by third parties on social media as, in the absence of some other factor or factors raising a reasonable expectation of privacy, it would seem that the tort would only apply where information that might be thought to be inherently private is misused.[179]

Another problem for an Australian employee hoping to establish a reasonable expectation of privacy in the context of employer surveillance may be that, at least if the US approach is adopted,[180] an employer would be able to destroy any such expectation by notifying the worker of the surveillance. Given the underlying inequality of bargaining power that often characterises the employment relationship, it may even be possible for any expectation to be removed through the employer obtaining the consent to that surveillance from the worker.[181] Moreover, in the US, even if an employee is able to show that an employer has intruded on their privacy, that intrusion is usually not considered highly offensive if the employer had a legitimate need for the information.[182] In Australia, the position might appear potentially more favourable to a worker, given that the ALRC ultimately rejected the 'highly offensive' test as too limiting to use in determining whether an invasion of privacy was serious under its proposed tort.[183] However, under the final element of the proposed tort, a worker would still

178 ALRC, *Serious Invasions of Privacy in the Digital Era*, above n 170, 82 [5.45].

179 As such, it would not, for example, protect a trainee solicitor facing dismissal following the posting of a video on YouTube in which drunk and apparently referring to his job, he states that he loves being 'a city lad' and 'fucking people over for money': Paul Wragg, Submission No 4 to Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, 4 <www.alrc.gov.au/sites/default/files/subs/04._p_wragg.rtf>, citing a 2013 media report of such a case in the UK.

180 The US courts have yet to acknowledge any core employee privacy expectations that cannot be destroyed by the use of notice or consent forms: see Lothar Determann and Robert Sprague, 'Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States' (2011) 26 *Berkeley Technology Law Journal* 979, 992.

181 The ALRC both suggested that consent would be relevant to the question of whether an individual had a reasonable expectation of privacy and recommended that it form the basis of a separate defence. While consent for these purposes must be freely given, Australian courts have generally been reluctant to recognise the element of implicit coercion that may exist in the employment relationship. See ALRC, *Serious Invasions of Privacy in the Digital Era*, above n 170, 96 [6.25], 195 (Recommendation 11–4), 198–9 [11.64]; Sempill, above n 85, 10–11, 31–2.

182 Robert Sprague, 'Invasion of the Social Networks: Blurring the Line between Personal Life and the Employment Relationship' (2011) 50 *University of Louisville Law Review* 1, 15.

183 ALRC, *Serious Invasions of Privacy in the Digital Era*, above n 170, 135 [8.23]–[8.24]. It recommended instead that a court have regard to, inter alia, 'the degree of any offence, distress or harm to dignity that the invasion of privacy was likely to cause to a person of ordinary sensibilities': at 132 (Recommendation 8–1).

be required to satisfy the court that the public interest in their privacy outweighed any countervailing public interest raised by the employer.[184]

Finally, any expectation of privacy is also relevant to the issue of the forced disclosure of passwords. In this regard, the ALRC has said that 'a password or some other form of personal identification … required to gain access to a digital location containing personal information … strongly suggests that the information is likely to be subject to a reasonable expectation of privacy'.[185] That said, even if a worker might have a reasonable expectation of privacy in the contents of their restricted social media page, by handing over passwords they might be taken to have consented to any invasion of privacy, and the ALRC has recommended that consent should provide a defence to any action based on its proposed tort.[186] However, given the fact that the recent Federal governments seem to have had little stomach for major legislative reform in this area,[187] there may be little chance that a new tort will be available to employees in the near future.

B *Workplace Privacy Regulator*

The VLRC recommended that '[a] statutory office of the workplace privacy regulator should be established'.[188] Currently, the state plays a relatively passive role around employer access of personal employee social media posts — only providing the forums of the Fair Work Commission and the Information Commissioner that allow individuals to seek redress. The VLRC proposal, while based on a 'light-touch' mode of regulation,[189] was aimed at emphasising compliance with the law while still providing for a complaints-resolution procedure.[190]

184 See ibid 132–3 [8.8]. An employer might also be able to avail itself of proposed defences under the tort. The two most relevant defences in this context would probably be consent (discussed above) and necessity. The latter defence would be available to an employer who could show that its conduct was 'incidental to the exercise of a lawful right of defence of persons or property … [and] proportionate, necessary and reasonable': ibid 191 (Recommendation 11–2).

185 Ibid 103 [6.60].

186 Ibid 195 (Recommendation 11–4). It may be noted that the Commission specifically addressed the question of 'unconscionable' employer demands for social media passwords in its Issues Paper for the *Serious Invasions of Privacy in the Digital Era* inquiry, though the ALRC did not return to this proposal in its Final Report: ALRC, *Serious Invasions of Privacy in the Digital Era*, Issues Paper No 43 (2013) 52 [180].

187 The Commonwealth Attorney-General, for example, responded to the issue of the ALRC's Discussion Paper in the *Serious Invasions of Privacy in the Digital Era* inquiry by saying: 'The government has made it clear on numerous occasions that it does not support a tort of privacy': Chris Merritt, 'Brandis Rejects Privacy Tort Call', *The Australian* (online), 4 April 2014 <http://www.theaustralian.com.au/business/legal-affairs/brandis-rejects-privacy-tort-call/story-e6frg97x-1226873913819?nk=25fd807edee43bd43>.

188 VLRC, above n 7, 93 (Recommendation 33).

189 Ibid 37.

190 Despite, or perhaps because of, the nature of the proposal, the VLRC's Recommendation has received very little academic attention; as an exception, Witzleb refers to the VLRC Report and the recommended regulator, specifically: Witzleb, above n 7, 146–7.

The regulator would have an educative function that would include the preparation of codes of practice. Some of these codes would be advisory, while others would be compulsory. The former 'could be drafted in a way which takes account of the needs and characteristics of different practices, different industries and different workplaces'.[191] The use of mandatory codes, on the other hand, was to be more restrictive. The VLRC only indicated, in keeping with the 'light-touch' approach,[192] two areas in which mandatory codes could be issued: 'covert surveillance' and the 'taking of bodily samples from workers or prospective workers'.[193] The latter, of course, has little relevance to social media posts; however, the former could cover covert employer monitoring of social media use. There could also be a compulsory code around requests for the disclosure of passwords.[194]

There are two arms of the proposed complaints-resolution procedure. The first is one that is focused on the complaint of an individual. Such a complaint could be made by a single worker, or by one worker on behalf of a number of workers. The second arm allows the regulator to investigate an employer beyond the confines of the matters raised in an individual complaint. To carry out such investigations, the regulator needs powers to obtain information and examine witnesses. The regulator would have the power to conciliate the complaint or make a ruling with respect to the actions of the employer (which could include ordering redress for any loss suffered by the worker).[195]

Finally, the VLRC recommended an authorisation procedure that is of specific relevance to this issue. The Recommendation was that, where an employer wished 'to engage in an act or practice which affects the privacy of a worker engaged in non-work-related activities', the employer needed the authorisation of the regulator. Further, before granting the request of the employer, the regulator needs to be 'satisfied that … there are reasonable grounds for believing the worker's out-of-hours activity may have a direct and serious impact on the business or reputation of the employer'. Further, the regulator needs to be satisfied that it is a 'proportionate response' and that the employer had informed and consulted its workers about the process.[196] Assuming that the social media use of the employee was on their own time, then it would appear that accessing employee social media posts would be covered by the Recommendation.

191 VLRC, above n 7, 56 [3.68].

192 The VLRC based their regulatory analysis on the work of Braithwaite: VLRC, above n 7, 114. They cite, for example, John Braithwaite, 'Responsive Business Regulatory Institutions' in CAJ Coady and CJG Sampford (eds), *Business Ethics and the Law* (Federation Press, 1993). As the title of that work suggests, the emphasis is on the regulation of the businesses and there is less conceptualisation of the employee from a regulatory perspective.

193 VLRC, above n 7, 61 [3.80].

194 Though, as noted above, the VLRC made no reference to social media in the Report.

195 For a more detailed discussion of the complaints procedure, and the specific Recommendations, see VLRC, above n 7, 96–112.

196 Ibid 73 (Recommendation 20).

C *Proposed Law from a Regulatory Perspective*

The discussion above showed that the current law is insufficient, from a regulatory perspective, to protect employees from the actions of employers. This section explores whether the two reforms discussed here fare any better. The differences between the current law and the proposed reforms can be understood in terms of the issue of norms and the changed role of the state.

The notion of 'expectation of privacy' and the regulatory technique of codes of conduct can both be seen in terms of norms. Both are standards that guide behaviour — with 'expectations' being the product of social forces and the codes the result of centralised action. With respect to the former, the new tort does not add significantly to regulation in the area. The litigation would still be founded on 'expectations' and a conflict over 'interests'.[197] There is no process for acknowledging the limits of the expectations nor for negotiating conflicts between expectations and workplace practices. Over time, judicial decisions may establish what reasonable expectations are for different practices (and possibly for different categories of employees). However, the processes of legal development take time — particularly as disputes may settle early (perhaps with an undertaking on the employer's part to desist from accessing social media posts) and, as a result, there may be few appellate decisions for a significant period of time.In addition, the longer it takes for the law to be established, the more likely it is that new disruptive technologies will be in use which may require a different set of legal standards.

The codes of conduct, assuming that they are the subject of consultation and negotiation, may be less one-sided and more relevant to particular industries. They would, in theory, clearly set out the limits of employer activities. Further, if the educative function of the regulator is carried out,[198] the justifications for the activities may be better communicated to the affected workers. The education should facilitate the internalisation of these standards by both sides. Such acceptance of the codes will decrease disputes. Of course, individuals — whether employers or employees — can choose to act against the accepted norms; however, this happens in all areas of law and regulation (individuals are, after all, not completely governable).

The codes will work most effectively if they are at least authorised by a body that is separate from the employers and the employees — to reduce the risk that either side will see a code as partisan. The VLRC's Workplace Regulator performs such a role. The inclusion of a public regulator, given the fact that the regulation of employer behaviour around employee social media posts already includes some public and some private aspects, would only represent a shift in the current blend of public and private regulation — rather than imposing a radical reorientation of the system. That is, the understanding of regulation offered here acknowledges the value in regulatory contributions from both spheres and does not consider

197 It would also be an expensive option and one that would impact significantly on the employment relationship.

198 VLRC, above n 7, 95–6.

that minimising the role of one or the other provides the most effective form of behavioural guides.

The acknowledgement of a role for a 'specialist' public entity in the regulation of behaviour has other effects. If, for example, one of the concerns over accessing social media posts is the fact that there may be no expectation of (full) privacy over them, then there may be cause to rethink the current public/private regulatory balance. That is, it may be that social media posts are best seen, and regulated, as public acts — despite the audience that the employee had in mind at the time of posting. If they are understood to be at least partially public, then there is the potential for a public regulator to have a bigger role. A regulator that is aware of, and caters to, the tension between the public and the private, within the act of posting itself, may support more effective regulation.

Assuming that both employers and employees are ungovernable, having a third entity — one that has legislated powers and limits (and, therefore, not ungovernable) — would have significant regulatory benefits. The inclusion of investigatory powers, beyond individual complaints, and the use of 'representative' complaints, broadens the dispute away from a single employee and their employer. This would remedy a number of the imbalances between the two parties. Further, the state power that underpins such a regulator would add force to restrictions on specific behaviours such as the forced disclosure of passwords. That said, the use of a state entity, as part of the mix of public and private regulation, would not be a resort to government control over the private sector. Instead, it would operate as one form of regulation amongst several. None of this is to say that the VLRC's proposal is perfect, or even politically feasible. The point here is that, from a regulatory-theoretical perspective, it resolves a number of problems in the current law and the proposal of a tort of privacy.

V CONCLUSION

It appears that an Australian employee who might be uncomfortable with their employer monitoring their personal life via social media may be able to do little more than adopt the maximum privacy settings available on any site they use and be careful whom they accept as an online friend. This is because Australian law — either workplace or privacy law — currently does little to stopemployers, particularly those in the private sector, from engaging in such practices. Given the fact that there is little specific legislation here, employees can be left vulnerable to the actions of employers given the underlying inequality of bargaining power that often characterises the employment relationship. Few would complain if an employer simply read a worker's tweet published as part of a televised debate; it is, nonetheless, likely that society does not want employers to peek into Grindr profiles, or to force everyone to use platforms, such as Snapchat, with time-limited posts.

The addition of regulatory theory to the analysis highlights particular concerns around the ungovernability of parties on both sides of the employment contract.

While this does not excuse the behaviour of either employers or employees, it provides an explanation of the difficulty of finding a solution. Of the two reforms considered here, it is the VLRC's workplace regulator model that best negotiates the tension around the accessing of personal employee social media posts. The downside, of course, is the greater expense involved in establishing the regulator and the legislative challenges around the constitutional limits of state and federal governments.