Author/s:
Blackham, A

Title:
Surveillance, Data Collection and Privacy at Work: A New Application of Equitable Obligations?

Date:
2025

Citation:
Blackham, A. (2025). Surveillance, Data Collection and Privacy at Work: A New Application of Equitable Obligations?. Australian Journal of Labour Law

Persistent Link:
https://hdl.handle.net/11343/353544

This manuscript has been accepted for publication in the *Australian Journal of Labour Law*. The published version of the work will be published by LexisNexis as Alysia Blackham, 'Surveillance, Data Collection and Privacy at Work: A New Application of Equitable Obligations?' (2025) *Australian Journal of Labour Law* (forthcoming).

SURVEILLANCE, DATA COLLECTION AND PRIVACY AT WORK: A NEW APPLICATION OF EQUITABLE OBLIGATIONS?

Alysia Blackham*

Abstract: Employers are gathering a sizeable body of employee data, some of which is sensitive and highly personal. However, privacy law in Australia remains fundamentally ill-adapted for protecting employee interests, due to significant exceptions for small businesses and employee records, and minimal protection of privacy rights at the federal level. Drawing on comparative doctrinal analysis of the UK and Australia, this article frames the dramatic regulatory gaps for employee data in Australia. It argues that equitable breach of confidence might prove to be a critical complement to the employment contract and other forms of legal regulation, to enable the protection of employees' sensitive data. This is particularly pertinent in jurisdictions like Australia, with limited statutory or human rights protection of privacy. However, it could also prove to be an important complement to other protections in jurisdictions like the UK, with statutory privacy law, human rights, contract law and equitable doctrines offering complementary protections.

I. INTRODUCTION

In 2022, there was nationwide news in Australia regarding a leak of employee records from Telstra, one of the nation's largest telecommunications companies.[1] The details of approximately 30,000 current and former employees, including their names and emails, were uploaded to an online forum soon after a customer data breach relating to the other major telecommunications provider (Optus). Both Telstra and NAB (one of the nation's major banks) had their employee data accessed via a 'third-party provider for an employee and member benefits program'.[2] The breach was downplayed, as it related to a third party's systems – not those of NAB or Telstra – the information was dated, and the data only consisted of employee names and email addresses – not dates of birth, and identification numbers, as in the Optus breach.

That said, only 12,800 of the 30,000 Telstra employees affected still worked at Telstra. Further, while the Optus customers would be protected by federal privacy law in Australia – the *Privacy Act 1988* (Cth) – employee records are largely exempt from privacy law in Australia. With no federal human rights act, minimal constitutional protection of rights, and no statutory or tortious right to privacy, employee data is minimally regulated in Australia. This differs markedly to the situation in the UK, where a right to privacy is embedded in the European

* Associate Professor, Melbourne Law School, The University of Melbourne; alysia.blackham@unimelb.edu.au
[1] Isabel McMillan and Eli Green, 'Major Bank Hit by Third Party Data Breach', *news.com.au* (online, 10 April 2022) <https://www.news.com.au/technology/online/hacking/telstra-reveals-data-breach-hit-30k-employees-after-optus-cyber-attack-reports-claim/news-story/437d4da4d44f560d3dfc9e692a85a301>.
[2] Ibid.

Convention on Human Rights (ECHR) art 8 and Human Rights Act 1998 (UK), and strongly regulated by UK privacy legislation (the Data Protection Act 2018 (UK) ('DPA') and UK General Data Protection Regulation (GDPR)).

While there is limited regulation of employee data and privacy at work in Australia, there is growing surveillance and aggregation of employee data. For many years, employers have been gathering a sizeable body of employee data, some of which is sensitive and highly personal.[3] While workplace surveillance well predates the explosion of digital technologies, it is being aided and expanded by new digital tools. For example, employees of the Commonwealth Bank of Australia (CBA) are required to download the 'Navigate' app to enter buildings, book a workstation, report a fault and register visitors. According to reviews of the app, the app collects employees' precise location data, at all times.[4] As one Google user noted in 2018: 'I'm really uncomfortable with the idea that this application requires 24/7 access to my location. A major privacy concern in my opinion'.[5] The app is being used to track staff movements, and CBA human resources are forcing workers to apply for leave when they appear 'unproductive' or are absent from their allocated workstation.[6] As the app's user reviews show, though, the app is unreliable and often fails to provide access to CBA offices. Collecting and relying on this data, including for performance processes, is therefore highly problematic, as it is potentially an invasion of employee privacy, and likely inaccurate.

In the face of widespread surveillance and employee data collection, an absence of statutory or constitutional regulation, minimal collective action, and limited contractual regulation, might equity offer a supplementary means of regulating employee data protection and privacy? Where a contract is silent regarding employee data and privacy, and privacy law offers little recourse, can equity's exclusive jurisdiction be used? This article argues that equitable breach of confidence might prove to be a critical complement to the employment contract and other forms of legal regulation, to enable the protection of employees' sensitive data. This is particularly critical in jurisdictions such as Australia, with limited statutory or human rights protection of privacy. However, it could also prove to be an important complement to other protections in jurisdictions such as the UK, with statutory privacy law, human rights, contract law and equitable doctrines offering complementary protections.

This article deploys comparative doctrinal analysis of the law relating to privacy, data protection and surveillance at work in Australia and the UK, to consider how equity and equitable breach of confidence might fill legal gaps. The UK and Australia share a common legal tradition, yet diverge markedly in this area of law and regulation. Explanatory comparative legal analysis therefore identifies similarities and differences across and between jurisdictions, and seeks to account for these variances.[7] This represents a 'problem-solving' or sociological approach to comparative law, examining how different legal systems have

[3] Kirstie Ball, 'Workplace Surveillance: An Overview' (2010) 51(1) *Labor History* 87 ('Workplace Surveillance'); Kirstie Ball, 'Surveillance in the Workplace: Past, Present, and Future' (2022) 20(4) *Surveillance & Society* 455 ('Surveillance in the Workplace').

[4] 'Navigate Now', *App Store* <https://apps.apple.com/au/app/navigate-now/id1262274260>.

[5] Review of Navigate Now 2.0 app, Google store, A Google User, 7 August 2018.

[6] 'CBA Using Productivity App to Spy on Staff', *Finextra Research* (15 March 2023) <https://www.finextra.com/newsarticle/41974/cba-using-productivity-app-to-spy-on-staff>.

[7] Maurice Adams, 'Doing What Doesn't Come Naturally: On the Distinctiveness of Comparative Law' in Mark van Hoecke (ed), *Methodologies of Legal Research: What Kind of Method for What Kind of Discipline?* (Hart, 2011) 229, 237.

responded to similar problems in contrasting ways.[8] The jurisdictions face similar challenges – of growing data collection and surveillance in the workplace – which justifies the comparison.[9] The dramatic differences between the jurisdictions increase the potential for mutual learning.[10] In particular, the comparative lack of regulation in Australia is revealed by the presence of regulation in other jurisdictions, such as the UK.

In Part II, I frame the regulatory gaps for employee data in Australia, focusing on federal and Victorian legislation, as well as protection offered via collective bargaining. In Part III, these gaps are contrasted with the human rights and data protection regimes in the UK, considering how these protections are being used in employment decisions to protect employee interests. In analysing these issues, my approach is doctrinal, but also socio-legal, reflecting a concern with both what law is (or might be) as well as with what law does (or might do).[11] In Part IV, I consider how equity – and, in particular, equitable breach of confidence – might fill these regulatory gaps in Australia, and complement existing protections in the UK. Part V concludes with a call to action for Australia.

II. AUSTRALIA: THE 'WILD WILD WEST' OF EMPLOYEE PRIVACY

A. Federal Regulation

Privacy is regulated at federal, state and territory level in Australia. At federal level, the *Privacy Act 1988* (Cth) creates thirteen Australian Privacy Principles (APPs) which regulate how personal information is collected, managed and used. The APPs create requirements for open and transparent management of personal information and anonymity; regulate the collection, use, and disclosure of personal information, including across borders; and make provision for access to and correction of information.

Federal privacy law applies to federal government entities and large organisations; most small organisations (with an annual turnover of AU$3 million or less) are exempt from regulation.[12] Small companies are not necessarily covered by state or territory privacy legislation, potentially creating a dramatic lacuna in privacy law for employees and customers of small businesses in some jurisdictions, with privacy law essentially not applying. This means, in essence, that privacy law does not apply to employees or customers of the vast majority of businesses in some jurisdictions: according to the Australian Bureau of Statistics (ABS), as at 30 June 2022, 92.6% of Australian businesses had less than AU$2 million in annual turnover (see Table 1). These statistics likely undercount very small businesses, as only those earning at least AU$75,000 annually need to register for GST (Goods and Services Tax), and the statistics only include those who are registered.[13]

---

[8] Esin Örücü, 'Developing Comparative Law' in Esin Örücü and David Nelken (eds), *Comparative Law: A Handbook* (Hart, 2007) 43, 52.
[9] Ibid.
[10] Dagmar Schiek, 'Enforcing (EU) Non-Discrimination Law: Mutual Learning between British and Italian Labour Law?' (2012) 28(4) *International Journal of Comparative Labour Law and Industrial Relations* 489, 508 ('Enforcing (EU) Non-Discrimination Law').
[11] Roger Cotterrell, *Law's Community: Legal Theory in Sociological Perspective* (Oxford University Press, 1997) 296.
[12] *Privacy Act 1988* (Cth) ss 6C(1), 6D.
[13] Australian Small Business and Family Enterprise Ombudsman, *Number of Small Businesses in Australia - August 2023* (2023) 4 <https://www.asbfeo.gov.au/sites/default/files/2023-10/Number%20of%20small%20businesses%20in%20Australia_Aug%202023_0.pdf>.

Annual turnover	Businesses in operation	% of all in operation
Zero to less than $50k	699,077	27.2
$50k to less than $200k	823,844	32.1
$200k to less than $2m	856,169	33.3
$2m to less than $5m	108,939	4.2
$5m to less than $10m	39,227	1.5
$10m or more	42,644	1.7
Total	**2,569,900**	100.0

Table 1: Businesses in operation by annual turnover ($AUD), 30 June 2022, Australia
Source: Australian Bureau of Statistics, 8165.0 Counts of Australian Businesses, including Entries and Exits, June 2018 to June 2022

Even for large businesses and federal public sector organisations captured by the Act, s 7B(3) of the *Privacy Act 1988* (Cth) contains an exemption in relation to employee records, where those records are directly related to a current or former employment relationship. 'Employee record' is defined broadly as 'a record of personal information relating to the employment of the employee'.[14] Examples of employee 'personal information' include health information, contact details, bank details, salary, sick leave, and tax details.[15] All of this is exempt from privacy law as part of an 'employee record'. In *Madzikanda v Australian Information Commissioner*,[16] then, the Australian Information Commissioner's decision not to investigate further an employer who allegedly accessed and used an employee's personal emails and personal passwords on a work laptop was upheld; the Commissioner saw the laptop, and all of its contents, as falling within the 'employee records' exemption, as it was subject to routine monitoring and review under the employer's policy.[17]

However, case law has clarified that the exemption for employee records only applies once those records are actually in existence; privacy law *does* apply to the initial collection of new employee data. In *Lee v Superior Wood Pty Ltd ('Lee')*[18] an employee was dismissed after failing to provide his fingerprint for an employer's new scanner, which was to be used at the beginning and end of each shift. The employer failed to comply with privacy law in various ways, including in relation to the (limited) information it provided to employees about how it would collect and handle their sensitive information: 'It merely informed them that the scanners were being introduced and that they would be required to use them.'[19]

The Full Bench of the Fair Work Commission (FWC) held that the s 7B(3) exemption of 'employee records' related to actual records already held by the organisation; it did not apply to records that did not yet exist.[20] This meant, then, that the employer *did* have to comply with

[14] *Privacy Act 1988* (Cth) s 6(1), definition of 'employee record'.
[15] Ibid s 6(1), definition of 'employee record'.
[16] [2023] FCA 1445.
[17] Ibid [16]. Even if the employee records exemption did not apply, there was held to be no breach of the APPs: [55].
[18] [2019] FWCFB 2946.
[19] Ibid [14].
[20] Ibid [55]–[56].

privacy law in soliciting and collecting new forms of data; but did not need to comply with privacy law once those records were collected.[21] This meant that the employer should have obtained Lee's 'genuine' consent to the collection of sensitive, biometric data; and consent obtained with the threat of dismissal or discipline could not be genuinely given.[22] The Full Bench also found that the collection of fingerprint data was not 'reasonably necessary' in accordance with APP 3 as other alternative sign-in options existed.[23] Overall, the Full Bench held that Mr Lee's dismissal was not for a valid reason, and was unjust. He had therefore been unfairly dismissed.[24]

Lee is revealing, too, in showing the flow of employee data, which is exempt from privacy law once collected. Data from the biometric scanners was:

- captured by Mitrefinch, a workforce management company;
- converted into a template using an algorithm owned by Lumidigm;
- then stored on site, as well as on servers owned by Finlayson Timber and Hardware Pty Ltd, a company related to Superior Wood; and
- could then be accessed by (at least) Finlayson Timber and Hardware Pty Ltd; Mitrefinch; AUS IT Services, a software company who operated the servers; and Ironbark, who operated the payroll system.[25]

There was no evidence that any of these various companies had measures in place to protect information in accordance with privacy law.[26] While large employers might need to comply with privacy law when collecting new employee data, there is little that restrains these data flows for data once it has been collected.

The validity of employee consent when given under threat of termination was further considered in *Construction, Forestry, Maritime, Mining and Energy Union v BHP Coal Pty Ltd* ('*BHP*').[27] In that case, BHP required employees to provide evidence of COVID-19 vaccination to access sites in Queensland. The unions argued these orders were invalid under the *Privacy Act 1988* (Cth), as 'any consent an employee may supply is vitiated by the threat that, if they do not consent, they may be disciplined or have their employment terminated'.[28]

Deputy President Asbury rejected this argument, and distinguished *Lee* on the facts.[29] In *Lee*, the employer had breached the *Privacy Act 1988* (Cth) in other ways, in that it failed to have a privacy policy; or issue a Privacy Collection Notice; or notify employees of required matters upon collecting personal information.[30] For Deputy President Asbury in *BHP*, any findings relating to the validity of consent in *Lee* were made in the context of those other breaches of the *Privacy Act 1988* (Cth).[31] These other aspects of non-compliance were not present in this case; therefore, for Deputy President Asbury, 'the decision in *Lee* turns on its own facts and is of limited relevance in [the] circumstances of this case'.[32] The economic and social pressure

[21] Ibid [57].
[22] Ibid [58].
[23] Ibid [85].
[24] Ibid [102].
[25] Ibid [99].
[26] Ibid [100].
[27] [2022] FWC 81.
[28] Ibid [68].
[29] Ibid [160].
[30] Ibid [162].
[31] Ibid [164].
[32] Ibid [166].

asserted by the employer in *BHP* did not amount to duress that could vitiate consent.[33] While employees who are directed to consent to provide sensitive information – under threat of termination – 'have a difficult decision to make', this does not amount to coercion or duress such that their consent is not legally effective.[34]

The decision in *BHP* reveals a far less substantive understanding of 'consent' in the employment relationship than that in *Lee*. 'Genuine' consent, under the threat of dismissal, appears illusory.[35] If followed in later cases, *BHP* is likely to further reduce the scope of privacy law to protect employee records and employee data. This might be compared with the approach in the EU: the European Data Protection Board (EDPB)[36] Guidelines 05/2020 on consent recognise that consent, in the employment relationship, is often not 'freely given' given the 'real risk' of detriment on refusal.[37] The EDPB therefore regards it as 'problematic' to rely on consent to justify data processing for current or future employees.[38] Employers should therefore only rely on consent as a basis for data processing at work in exceptional cases, where consent actually is freely given, and there are no adverse consequences for withholding consent.[39] This contrasts markedly to the approach in *BHP*.

In the relative absence of regulation by privacy law, unfair dismissal claims might provide a forum to challenge employer surveillance, though only after a dismissal has occurred. However, in *Cheikho v Insurance Australia Group Services Ltd* ('*Cheikho*')[40] an employer's use of employee monitoring software on a work computer was implicitly upheld in an unfair dismissal claim. Ms Cheikho worked remotely. She was dismissed for misconduct, for a failure to work as required between October and December 2022. The evidence of misconduct was a review of Ms Cheikho's cyber activity, including key-stroke activity and log-ins. The cyber review measured Ms Cheikho's productivity on an hourly and daily basis, and revealed that Ms Cheikho often logged in late, logged off early, and had 320 hours with zero keystroke activity over this period.[41] Ms Cheikho reported being 'confused and shocked when presented with the data',[42] but the evidence was accepted by the Fair Work Commission as being a valid reason for dismissal.[43] There was seemingly no need to consider how the data was collected, whether Ms Cheikho was notified or consented to the software being used, or whether this was consistent with privacy law or rights to privacy.[44]

---

[33] Ibid [171].
[34] Ibid [171].
[35] See, eg, Jeremias Adams-Prassl et al, 'Regulating Algorithmic Management: A Blueprint' (2023) 14(2) *European Labour Law Journal* 124, 132–3 ('Regulating Algorithmic Management'); Alysia Blackham, 'Setting the Framework for Accountability for Algorithmic Discrimination at Work' (2023) 47(1) *Melbourne University Law Review* 63, 84–86.
[36] The EDPB is tasked with ensuring the GDPR is applied consistently across countries, and can issue guidelines to clarify the GDPR.
[37] European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679*, Version 1.1 (adopted 4 May 2020) [21] <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 27 May 2024.
[38] Ibid.
[39] Ibid [22]. See also the earlier Article 29 Data Protection Working Party, *Opinion 8/2001 on the processing of personal data in the employment context*, adopted on 13 September 2001, 5062/01/EN/Final WP48; Article 29 Data Protection Working Party, *Opinion 2/2017 on data processing at work – WP249* (8 June 2017).
[40] [2023] FWC 1792.
[41] Ibid [21].
[42] Ibid [25].
[43] Ibid [30].
[44] Though Ms Cheikho was self-represented, and may have raised these points if she had legal representation.

In *Lee*, while it was not possible to gather sensitive biometric data without consent, it was possible to track employees' movements at work, and to use alternative methods – like paper records or other tools – to require employees to sign in and out. In *BHP*, the collection of vaccination data was seen as a reasonable means of managing and minimising the health and safety risks of contracting COVID-19 at work. In *Cheikho*, the employer was able to monitor keystrokes, logins, and overall productivity on a work computer, to manage work performance. These are forms of employee data collection that might be seen as reasonable and necessary for employers to manage work performance, safety and productivity. These forms of data would likely be covered by APP 3.2, which says that, for organisations, 'the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.' The collection of sensitive information also generally requires consent under APP 3.3. The test of reasonable necessity could offer an important touchstone for establishing what data employers should, and should not, collect and hold about employees. For example, it is likely not reasonably necessary to gather employee location data outside of work hours, or to retain employee data years after the employment relationship has ended. At present, however, even these limitations likely do not apply to existing employee records.

As well as limited statutory regulation, there is no federal human rights act or legislation in Australia, and the minimal protection of individual rights in the Australian Constitution does not extend to privacy. Protection of privacy, particularly in the workplace, is therefore limited at the federal level. Prompted by the growth of online platforms, and fears for consumer data protection,[45] the Australian government has conducted a broad review of federal privacy law.[46] In 2023, in response to the findings of that review, the government agreed in principle to removing the small business exception, subject to further consultation.[47] The government also agreed in principle to conduct further consultation on the employee records exemption,[48] though did not commit to its removal or modification. The Australian Human Rights Commission has also called for a federal human rights act, which would include a right to privacy.[49] This proposal has been endorsed by the Parliamentary Joint Committee on Human Rights, including due to concerns that privacy is not adequately protected in Australia.[50] Eventually, legislative reform may help address some of the most glaring gaps in employee data protection in Australia. Until then, though, other potential avenues need to be considered.

B. State Regulation

[45] Australian Competition and Consumer Commission, *Digital Platforms Inquiry - Final Report* (June 2019) 3 <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf>.

[46] Attorney-General's Department, *Privacy Act Review - Discussion Paper* (October 2021) 217 <https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review-discussion-paper.pdf>; Attorney-General's Department, *Privacy Act Review Report 2022* (2022) <https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf>.

[47] Attorney-General's Department, *Government Response - Privacy Act Review Report* (2023) 6 <https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF>.

[48] Ibid.

[49] Australian Human Rights Commission, *A Human Rights Act for Australia: Position Paper: Free and Equal* (December 2022) <https://humanrights.gov.au/sites/default/files/free_equal_hra_2022_-_main_report_rgb_0_0.pdf>.

[50] Parliamentary Joint Committee on Human Rights, *Inquiry into Australia's Human Rights Framework* (May 2024) [4.43]–[4.46] <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/HumanRightsFramework/Report>.

At the state level, privacy law is largely confined to state government entities. In Victoria, for example, the *Privacy and Data Protection Act 2014* (Vic) contains ten Information Privacy Principles (IPPs) that regulate Victorian public sector organisations.[51] The Act does not cover private organisations unless they are a contracted service provider to the State, and then only in relation to their provision of services under that contract,[52] and only if the contract requires compliance with the IPPs.[53] The *Surveillance Devices Act 1999* (Vic) also regulates surveillance devices in the workplace, but only to prohibit the knowing use of optical surveillance or listening devices in workplace toilets, washrooms, change rooms or lactation rooms.[54] Otherwise, surveillance is acceptable with express or implied consent.[55] That said, employee health information – held by employers in both the public and private sectors – is regulated by the *Health Records Act 2001* (Vic).

Victoria is one of the few Australian jurisdictions with a statutory human rights instrument (along with Queensland and the Australian Capital Territory). The *Charter of Human Rights and Responsibilities Act 2006* (Vic) (the Charter) includes a right to privacy: s 13 says

> A person has the right not to have that person's privacy, family, home or correspondence unlawfully or arbitrarily interfered with.[56]

However, the Charter is grounded in a 'dialogue' model, which focuses on statutory interpretation by the courts,[57] parliamentary deliberation[58] and the acts of public authorities.[59] Only public entities are bound by the Charter,[60] and the Charter makes only limited provision for individual enforcement. Individual Charter complaints can only be made where attached to some other legal claim – a 'piggy back' enforcement model.[61] Remedies for breach of the Charter do not include damages.[62] As a result, claims under the Charter are rare,[63] and the Charter has had less influence on the development of individual privacy rights than in other jurisdictions like the UK.

In *Jurecek v Director, Transport Safety Victoria*[64] the Victorian Supreme Court considered the implications of the Charter for the interpretation of privacy law in the employment context. In that case, a public authority had used an employee's private social media postings as part of disciplinary proceedings. The employee argued this was a breach of the IPPs, as she was not given notice of the use of social media, and the information should have been obtained from her directly. A Charter complaint was not made, but the Charter was relevant to how the IPPs were interpreted. Thus, the definition of 'personal information' in the IPPs was 'interpreted beneficially and compatibly with human rights'.[65] While the claimant's social media posts were

[51] *Privacy and Data Protection Act 2014* (Vic) s 13.
[52] Ibid s 13(1)(j).
[53] Ibid s 17(2).
[54] *Surveillance Devices Act 1999* (Vic) s 9B.
[55] Ibid ss 6, 7, 8.
[56] *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 13(a).
[57] Ibid ss 32–37.
[58] Ibid ss 28–31.
[59] Ibid s 38.
[60] Ibid ss 6(2), 4.
[61] Ibid s 39(1).
[62] Ibid s 39(3).
[63] Though see, eg, *Loielo v Giles* [2020] VSC 722; *Thompson v Minogue* [2021] VSCA 358.
[64] [2016] VSC 285.
[65] Ibid [77].

held to be 'personal information',[66] which were not generally available publications,[67] and therefore within the scope of privacy law, the Court held there was no breach of the IPPs, as the collection of the information was 'necessary' for the public authority's functions[68] and the disciplinary process.[69]

C. Collective Bargaining

Even in the absence of statutory or constitutional protection for privacy, regulation might emerge via collective bargaining. However, collective regulation of privacy and employee data appears to be fairly under-developed. Searching the Fair Work Commission's document database of approved enterprise agreements[70] – 158,599 agreements as at 19 October 2023 – 29,984 agreements mention 'privacy', but only 288 agreements include the term 'employee privacy'. Many of these 288 agreements relate to the mining or construction industry, perhaps reflecting the prevalence of worker drug testing in the mining industry in particular, as one strategy for managing the health and safety risks of drug consumption on site.[71] No enterprise agreements included the terms 'employee data' or 'employee information'.

Some agreements reference employee privacy in relation to managing family violence leave.[72] Other agreements contain more fulsome provisions relating to privacy, particularly relating to employee health information (again, on mine sites): for example, the *Port Operations - Mount Isa Mines Limited Enterprise Agreement 2011* says in clause 6.10:

> The Company is bound by the Privacy Act 1998 (Cth) and the National Privacy Principles contained within that Act.
>
> The employees acknowledge that the Company may require personal and/or health information relevant to their employment with the Company in order to manage the business of the Company and administer it's [sic] obligations as an employer as such employees:
>
> (i) May be required to provide the company with personal and/or health information, relevant to the employees employment with the company, from time to time;
> (ii) acknowledge that the relevant personal and/or health information may be used by the Company, and consent to such use, for any reasonable purpose related to their employment with the Company, including without limitation their assessment of fitness for work and their safety in the environment in which they work;
> (iii) consent to the Company disclosing such relevant personal and/or health information about the employee to its advisors, related entities or other persons if such disclosure is reasonably necessary for a purpose related to his/her employment with the Company.
>
> A failure to provide relevant personal and/or medical (including pre-existing) health information requested by the Company may amount to misconduct. An employee may gain access to the

[66] Ibid [80].
[67] Ibid [83]–[84].
[68] Ibid [103]–[104].
[69] Ibid [121].
[70] Fair Work Commission, 'Document Search' <https://www.fwc.gov.au/document-search?q=*&options=SearchType_3%2CSortOrder_agreement-date-desc>.
[71] See, eg, Occupational Health and Safety Regulations 2017 (Vic) reg 409.
[72] Whitehorse Manningham Regional Library Corporation Enterprise Agreement 2022 cl 22.4; Ramsay Health Care Victoria Health Professionals Enterprise Agreement 2023 cl 6.12.

> personal information held about themselves by contacting the Human Resources Department … and complying with the requirements for satisfying the conditions of such access.

This clause pre-dates the decision in *Lee*. Following *Lee*, it is unclear whether 'collective consent' – in an enterprise agreement, which can bind employees who do not vote in favour of the agreement – is sufficient for the collection of this sort of data. More likely, individual consent will also need to be obtained if new data is collected. This likely remains the case after *BHP.*

More recent enterprise agreements also touch on surveillance as part of their privacy provisions. For example, the *Service Stream CFMEU and AMWU Yallourn Power Station & Open Cut Mine 2023* says in clause 40:

> The Power Station represents Critical Infrastructure and as such, its security and that of its workers and other parties may require surveillance or monitoring. However, the Company also recognises the right of Employees to be able to work free from unreasonable intrusions into their personal privacy.
>
> To this end electronic installations for site gate access, Cardax and security cameras, shall not be used for timekeeping or Employee surveillance other than to investigate any reasonable suspicion of serious misconduct or unlawful activity.
>
> The Company will display signage in areas of the workplace where there are overt surveillance devices under its control in operation. Covert surveillance will only be conducted in accordance with the applicable legislation.
>
> The IT environment and its usage will be physically and electronically monitored to ensure legal, ethical and operational compliance. This clause is subject to reasonable client requirements for monitoring and surveillance of its facilities.[73]

These clauses attempt to balance surveillance, data collection and employee privacy: by limiting the requirement to provide personal data to what is 'relevant' to employment, and limiting disclosure to other parties to what is 'reasonably necessary', in the *Port Operations - Mount Isa Mines Limited Enterprise Agreement 2011*, for example; and by attempting to create a degree of personal privacy in the workplace, including from covert surveillance, in the *Service Stream CFMEU and AMWU Yallourn Power Station & Open Cut Mine 2023* agreement.

The difficulty, though, is that there is minimal statutory guidance at the federal level as to how this balance should be struck, at least for the majority of companies not covered by privacy law. Different companies and agreements will conceive of the nature and boundaries of employee 'privacy' differently. The question remains, then: where should the boundaries of 'employee privacy' be, recognising employers' legitimate interests in collecting some types of employee data? What is – or should be – 'privacy' at work? The UK offers some guidance as to how this balance might be struck.

III. THE UK: DATA REGULATION AT WORK

Unlike in Australia, in the UK employee data and surveillance is regulated via a range of regulatory tools, including the DPA, the UK GDPR and the Human Rights Act 1998 (UK),

[73] A similar clause appears in EnergyAustralia Yallourn Enterprise Agreement 2023 cl 26.

which gives effect to the ECHR. The UK therefore offers critical insights into both how these issues might be regulated, and the possible impacts of regulation on the workplace specifically.

Article 8 of the ECHR provides that: 'Everyone has the right to respect for his private and family life, his home and his correspondence.'[74] 'Private life' in art 8 is not confined to the home; it may include professional activities or those in a public context.[75] Personal communications in the workplace might also be protected.[76] Article 8 has therefore been held to create a positive obligation on states to protect the right to private life in relation to workplace monitoring.[77] Atkinson argues that the decision of the Grand Chamber of the European Court of Human Rights in *Barbulescu v Romania*[78] 'breaks new ground by recognising an irreducible core to the right to private life in the workplace, which does not depend on an employee's reasonable expectations and cannot be eliminated by internal company policies.'[79] Workplace monitoring – even on a work computer – might therefore infringe the right to respect for private life and correspondence in art 8.[80]

And yet, human rights (and, in particular, the right to respect for private life) are only occasionally invoked in Employment Tribunal (ET) decisions in Great Britain. In a search of the ET website on 10 November 2023,[81] which captures decisions from February 2017 on, of 105,839 decisions, only 260 made explicit reference to the "European Convention on Human Rights"; 340 referred to the "ECHR". While the search function for ET decisions is fairly basic, only seven decisions referred to "art 8" and privacy;[82] all related to anonymity orders. Of the 257 decisions that referred to "article 8" and privacy, all also referred to "anonymity". Article 8 seems most often pertinent, then, when considering whether to impose anonymity orders.[83] It seems to be doing less work in determining the rights and obligations of parties to the employment contract, at least in ET decisions.

The *Data Protection Act 2018* (UK) (DPA) generally applies to employment and employee records. The DPA supplements the UK GDPR.[84] It creates obligations for data controllers to only collect and process personal data in ways that are transparent and necessary[85] and to secure

[74] On the application of art 8 to workplace monitoring, see *Halford v UK* [1997] ECHR 32; *Copland v UK* [2007] ECHR 253.
[75] *Barbulescu v Romania* App no. 61496/08 (ECtHR, 5 September 2017) [71].
[76] Ibid [72], [81].
[77] Ibid [111]–[112]; see Joe Atkinson, 'Workplace Monitoring and the Right to Private Life at Work' (2018) 81(4) *The Modern Law Review* 688.
[78] App no. 61496/08 (ECtHR, 5 September 2017).
[79] Atkinson (n 77) 697.
[80] See, eg, *Barbulescu v Romania* App no. 61496/08 (ECtHR, 5 September 2017).
[81] 'Employment Tribunal Decisions', *GOV.UK* <https://www.gov.uk/employment-tribunal-decisions>.
[82] *Z v Network Rail Infrastructure Ltd* [2023] UKET 2200397/2023; *Avdonina v Delin Capital Asset Management UK Ltd* [2021] UKET 2206956/2018; *Akhigbe v St Edward Homes Ltd* [2021] UKET 2303263/2018; *Haydari v Narvar UK Ltd* [2023] UKET 2206629/2022 and 2206631/2022; *Hudson v Home Office* [2019] UKET 3328288/2017; *Cuases v Evans* [2020] UKET 2201013/2019. In one case, the ET omitted details of the claimant's condition to minimise interference with the right to private life: *Modeste v Barclays Bank (UK) plc* [2022] UKET 4102303/2019.
[83] See, eg, *Ithia v MUFG Securities EMEA plc* [2023] UKET 2206616/2020; *Leeks v King's College London Hospital NHS Foundation Trust* [2022] UKET 2302989/2017.
[84] *Data Protection Act 2018* (UK) ss 1, 4. The UK GDPR is the GDPR as it applied to the UK on the date the UK withdrew from the EU: s 3(10).
[85] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (UK GDPR) art 5, 6.

such data.[86] It restricts automated processing[87] and creates rights to information,[88] access,[89] rectification[90] and erasure for personal data.[91] Where processing 'is likely to result in a high risk to the rights and freedoms of natural persons', controllers must conduct a data protection impact assessment prior to processing, to assess risks and safeguards in place.[92] Personal data breaches that pose a risk to the rights and freedoms of natural persons must be reported to the Information Commissioner[93] and, where the risk is high, the data subject must also be notified.[94] The scope of the DPA is broad, and – like the UK GDPR – includes workplace processing.[95] Breach of the DPA can lead to remedies[96] including compensation[97] for those affected, and significant administrative fines.[98]

While applicable to the employment context, the DPA is having only limited impact on decisions relating to employment rights handed down by ETs, perhaps reflecting the focus on enforcement by the Information Commissioner.[99] A search of ET decisions conducted on 14 November 2023 identified 105,890 reported decisions, with only 62 of those decisions referring to the "Data Protection Act 2018". ET decisions often referred to the DPA in the context of claimants making data subject access requests,[100] or where an employee had dealt with data in a way that allegedly contravened the DPA, often leading to dismissal.[101] In some cases, issues relating to the DPA were struck out as the ET did not have jurisdiction to hear them.[102]

It is more common for ET decisions to refer to the GDPR: in a search conducted on 24 May 2024 of 111,845 decisions, the GDPR was mentioned in 524 decisions.[103] In multiple cases, claimants alleged that the reason for their dismissal was because they made protected disclosures relating to the respondent's GDPR non-compliance[104] (which was unrelated to

[86] Ibid art 25, 32.
[87] Ibid art 22.
[88] Ibid art 13, 14.
[89] Ibid art 15.
[90] Ibid art 16.
[91] Ibid art 17.
[92] Ibid art 35.
[93] Ibid art 33.
[94] Ibid art 34.
[95] *Data Protection Act 2018* (UK) s 4; UK GDPR art 2.
[96] UK GDPR art 79.
[97] Ibid art 82.
[98] Ibid art 83.
[99] See, eg, the discussion in *Baig*, where it was made clear that the ET had no jurisdiction to deal with a claim for breach of the DPA or GDPR: *Baig v Harneys Westood Reigels LLP* [2022] UKET 3200847/2021 [20] (23 August 2022).
[100] See, eg, *C v Browns Food Group Ltd* [2023] UKET 8000075/2023 (13 October 2023); *Kahn v Johnson and Johnson Medical Ltd* [2019] UKET 1811024/2018 (11 June 2019); *Lee v Splunk Services UK Ltd* [2020] UKET 2205740/2018 (21 July 2020); *Wordsworth v Medical and Legal Admin Services Ltd* [2021] UKET 1804999/2020 (16 December 2021); *Alexander v Imperial College Healthcare NHS Trust* [2021] UKET 2206345/2021 (14 November 2022); *Savva v Leather Inside Out* [2023] UKET 2207192/2020 (4 August 2023).
[101] See, eg, *Barry v AmTrust Management Services Ltd* [2023] UKET 2202261/2019 and 2203325/2019 (24 September 2020); *Holt v London Borough of Haringey* [2022] UKET 3301964/2020 and 3307354/2020 (12 October 2022) [202], [208]–[209].
[102] *Hu v Recroot Ltd* [2022] UKET 2603154/2021 (13 July 2022). See also *Alexander v Imperial College Healthcare NHS Trust* [2021] UKET 2206345/2021 (14 November 2022).
[103] Some decisions make no reference to the GDPR, yet are picked up in the search results; it is unclear why the search engine is identifying these decisions: see, eg, *Thornton v IBM UK Ltd* [2019] UKET 1403981/2018 (22 November 2019).
[104] *Ford v Alfresco Concepts (UK) Ltd* [2021] UKET 1400374/2019 (4 July 2021); *di Fiore v Introhive UK Ltd* [2021] UKET 2203125/2020 and 2203126/2020 (5 November 2021); *Cheng v Garic Ltd* [2023] UKET

employee data). Overall, 152 of the GDPR cases related to public interest disclosures. In other cases, employees had been dismissed (in whole or part) due to non-compliance with the GDPR;[105] 350 of the cases were in the unfair dismissal jurisdiction.

That said, there were instances in these cases where employees had attempted to challenge employers' data protection practices relating to employee data. For example, the DPA was raised by a claimant seeking (unsuccessfully) to challenge their employers' COVID masking and testing policies, though the DPA did not weigh strongly in the ET's decision-making in that case.[106] In *Jovcic-Sas v Bath College*,[107] the claimant raised a number of concerns about the employer's data practices, including in relation to the collection of employee health data to evaluate COVID-19 risks. Following this, though, the employer also raised concerns about the employee's handling of data, including in failing to delete incompletely redacted material she had been asked to delete (and lying that she had done so). The employee's handling of data ultimately was the reason given for the employee's dismissal, which was upheld by the ET.[108] This case perhaps illustrates the double-edge sword of data protection law for employees; it can be both protective, and create grounds for dismissal.

Similarly, in *Murray v The Chief Constable of Thames Valley Police*,[109] the employee raised concerns regarding how the employer handled employee sickness data, and how sensitive data was discussed in meetings. While the ET held that the claimant had made protected disclosures relating to these data management processes, any adverse treatment was held not to be because of those protected disclosures. In *Wakefield v Adomast Manufacturing Ltd*,[110] the claimant was also held to have made protected disclosures relating to data practices.[111] However, the protected disclosures were not 'the operative cause of the respondent's decision to dismiss the claimant'; rather, the working relationship had broken down for personal reasons.[112] The claim of unfair dismissal was therefore rejected.[113]

Overall, then, data protection and privacy law appears to be having only a limited impact on ET decisions. The exception to this is in the case of *Tilli v Fresh & Wild Ltd T/a Whole Market Foods* ('*Tilli*'),[114] a case of constructive dismissal. In that case, the ET held that while the GDPR and DPA created obligations for the employer, the GDPR and DPA did not form part of the employee's contract of employment; there was no express contractual term to that

2408057/2021 (7 December 2023). This claim was upheld in *Stead v Ligman Ltd* [2021] UKET 2300258/2019 (30 March 2021).

[105] *Boucher v Essential Finance Group (UK) Ltd* [2022] UKET 2407283/2021 (6 June 2022); *Ready v Nottinghamshire Independent Domestic Abuse Service* [2021] UKET 2600687/2020 (22 March 2021); *McCann v Acorn Care and Education Ltd* [2021] UKET 2410201/2019 (25 January 2021); *Keir v Securitas Security Services (UK) Ltd* [2021] UKET 4109967/2021 (13 December 2021).

[106] See, eg, *Onyebalu v The Governing Body of Gascoigne Primary School* [2023] UKET 3205347/2021 and 3200006/2022 (4 October 2023).

[107] [2023] UKET 1403002/2021 (22 June 2023).

[108] Ibid [4.85]–[4.87], [4.117].

[109] [2023] UKET 3315333/2020 (21 August 2023).

[110] [2021] UKET 1801196/2020 (27 January 2021).

[111] Ibid [259].

[112] Ibid [269].

[113] Ibid [270]; cf *Goburdhun v Stuart Harris Associates Ltd* [2022] UKET 3300204/2021 (10 March 2022), where the claim of unfair dismissal was upheld. The claimant's accessing of client records was held not to be gross misconduct, as she had a 'legitimate interest' in the data in responding to disciplinary proceedings against her, making a complaint to the Association of Chartered Certified Accountants against her employer, and in pursuing the ET proceedings: at [119].

[114] [2022] UKET 2204611/2019 (9 May 2022) (*Tilli*).

effect.[115] However, the respondent conceded that a breach of the GDPR or DPA could 'in principle be relevant to whether there has been a breach of the implied term of trust and confidence in this case, and that a sufficiently serious breach of the GDPR/DPA may of itself amount to a breach of the implied term of trust and confidence',[116] and could also amount to a breach of art 8.[117] (Again, this reinforces the gaps in Australian labour law, where – in addition to the absence of rigorous data protection regulation, and any federal equivalent to art 8 – an implied term of trust and confidence in employment contracts has not been accepted by the courts.)[118]

In *Tilli* the privacy issues related to the use of CCTV surveillance of employees at Whole Foods Market (a supermarket owned by Amazon). The employer used CCTV repeatedly to monitor the claimant's interactions with customers (and thereafter criticised her for talking to a customer for too long),[119] to check back on the claimant's interactions with customers,[120] and to check on the claimant's health condition and disability.[121] The claimant lodged a complaint with the Information Commissioner's Office (ICO); the ICO accepted, in principle, that 'an employer may have a legitimate interest in processing personal data for purposes of performance management and disciplinary, grievance and other investigations.'[122] The ET agreed with this conclusion.[123] However, the ICO also expressed a view that personal data obtained for one purpose should generally not be used for other purposes without notice; to do so would be 'unfair'.[124]

In *Tilli*, the respondent's policies only related to the monitoring of employee use of information systems; it did not mention or encompass monitoring via passive systems such as CCTV.[125] Drawing on the respondent's Handbook provisions,[126] the ET held that the respondent's policy was that 'its purpose in collecting CCTV data is to protect customers and Team Members and discourage theft or robbery'.[127] The use of CCTV for performance or disciplinary investigations was therefore a breach of arts 5(1)(a) and (b) of the GDPR. The ET held that 'unfair use of the CCTV data has been made by using it for purposes other than that which employees have been told it will be used for'.[128] The ET also held that the use of CCTV went beyond what was 'necessary' to investigate the minor performance issues raised, and therefore breached art 5(1)(c) of the GDPR.[129]

---

[115] Ibid [229].
[116] Ibid.
[117] Ibid [230].
[118] *Commonwealth Bank of Australia v Barker* (2014) 253 CLR 169. See, eg, Vanitha Sundra-Karean, 'The Erosion of the Implied Term of Mutual Trust and Confidence in Australian Employment Law: Are Common Law and Statute Necessarily Uncomfortable Bedfellows?' (2016) 45(4) *Common Law World Review* 275 ('The Erosion of the Implied Term of Mutual Trust and Confidence in Australian Employment Law').
[119] *Tilli v Fresh & Wild Ltd T/a Whole Market Foods* [2022] UKET 2204611/2019 (9 May 2022) [54].
[120] Ibid [84].
[121] Ibid [102].
[122] Ibid [250].
[123] Ibid.
[124] Ibid.
[125] Ibid [252].
[126] Ibid [253].
[127] Ibid [254].
[128] Ibid [254], [256].
[129] Ibid [257].

In this case, the ET held that the GDPR breaches and use of CCTV were serious enough, of themselves, to breach the implied term of trust and confidence.[130] The claimant was therefore constructively dismissed.[131] The ET particularly noted the highly intrusive and damaging nature of using CCTV footage for employee surveillance, 'as it captures data that is very personal to the individual even when they are moving in a public space or a workspace.'[132]

These ET cases, taken together, indicate that multiple employees, across different workplaces and industries, are making protected disclosures relating to data protection; however, this is more commonly associated with consequences for the employee (and often flagged in unfair dismissal cases) than for the employer. The exception to this trend is in *Tilli*, where the claimant's claim for constructive dismissal was upheld on the basis of the employer's unlawful surveillance.

IV. EQUITABLE BREACH OF CONFIDENCE AND DATA PROTECTION

In the face of limited statutory regulation, and limited collective regulation through enterprise agreements, might private law – and, more specifically, equity – be used to strengthen employee data protection? What role might equitable breach of confidence play in developing the employment contract? These questions are critical in Australia, given the prevailing regulatory gaps. But they are also pertinent in the UK, despite existing privacy regulation and human rights protection. In the UK, equity might offer complementary protections to other legal regulation, as explored below.

This approach reflects equity's ability to 'evolve over time as circumstances change',[133] particularly where the law is otherwise inadequate to protect the rights in question.[134] Indeed, while the Australian High Court did not accept 'an emergent tort of invasion of privacy' in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* ('*Lenah Game Meats*'),[135] Gummow and Hayne JJ did not preclude the potential development of equity to better protect individual privacy.[136] As Kirby J opined: 'equity is a living force and … responds to new situations. … If it were to fail to respond, it would atrophy.'[137] In *Smethurst v Commissioner of Police (Cth)* ('*Smethurst*')[138] arguments based on a tort of invasion of privacy were not pursued by the parties, but were seemingly left open to further development by the High Court.[139] Edelman J also raised the possibility of an incremental extension and development of equitable principles 'to further an underlying principle of privacy'.[140]

Thus, while the High Court's approach in *Lenah Game Meats* and *Smethurst* arguably reflects a cautious approach to the development of the law, which may confine judicial development of equitable principles, at least some members of the Court appear open to the development and incremental extension of equity to better protect individual privacy. In this context,

[130] Ibid [258], [266].
[131] Ibid [266].
[132] Ibid [258].
[133] *Wolverhampton City Council v London Gypsies and Travellers* [2023] UKSC 47, [19] (Lord Reed, Lord Briggs and Lord Kitchin, with whom Lord Hodge and Lord Lloyd-Jones agree).
[134] Ibid [238] (Lord Reed, Lord Briggs and Lord Kitchin, with whom Lord Hodge and Lord Lloyd-Jones agree).
[135] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199.
[136] Ibid 258 (Gummow and Hayne JJ).
[137] Ibid 271 (Kirby J) (references omitted).
[138] (2020) 272 CLR 177.
[139] Ibid 206, 217–8 (Kiefel CJ, Bell and Keane JJ), 232 (Gageler J), 257 (Gordon J), 260, 271–3 (Edelman J).
[140] Ibid 272–3 (Edelman J).

developing the role of equitable breach of confidence to better protect employee data could be seen as a principled and incremental development of existing equitable rules.

A. Equitable breach of confidence

Equity imposes a duty of confidence on those who receive confidential information, where they knew or ought to have known that information was 'fairly and reasonably to be regarded as confidential'.[141] The duty will be breached when the information is used in a way inconsistent with the confidential nature of that information. Breach can lead to a range of remedies, such as an injunction to restrain inconsistent use or further threatened inconsistent use of the information;[142] delivery up or destruction;[143] account of profits;[144] or equitable compensation.[145] Where information has already been released, damages might also be available for distress, including aggravated damages (though this is contentious),[146] and damages under the Lord Cairns' Act might be available, even without economic loss.[147]

Gummow J in *Smith Kline & French Laboratories (Aust) Ltd v Secretary, Department of Community Services & Health* ('*Smith Kline*')[148] summarised the elements of the equitable obligation of confidence as being:

> (i) the plaintiff must be able to identify with specificity, and not merely in global terms, that which is said to be the information in question, and must be able to show that;
> (ii) the information has the necessary quality of confidentiality (and is not, for example, common or public knowledge);
> (iii) the information was received by the defendant in such circumstances as to import an obligation of confidence,
> (iv) there is actual or threatened misuse of that information, without the consent of the plaintiff. [149]

In the UK, art 8 has spurred the development of equitable breach of confidence: as Lord Nicholls has concluded, 'the values enshrined in articles 8 and 10 are now part of the cause of action for breach of confidence'.[150] Bryan and others argue that the equitable obligation of confidence now revolves around two aspects: protecting commercially valuable information; and protecting personal, private information.[151] A key aspect of the equitable obligation of confidence is the degree to which it potentially overlaps with other, non-equitable doctrines and obligations;[152] this is considered further below.

---

[141] *Campbell v MGN Ltd* [2004] UKHL 22, [14] (Lord Nicholls); *Trailfinders Ltd v Travel Counsellors Ltd and Ors* [2020] EWHC 591 (12 March 2020) [118].
[142] *Bluescope Steel Ltd v Kelly* (2007) 72 IPR 289, [157].
[143] *Franklin v Giddins* [1978] Qd R 72, 83; *NP Generations Pty Ltd v Feneley* (2001) 80 SASR 151, [33].
[144] *Bluescope Steel Ltd v Kelly* (2007) 72 IPR 289, [16]–[174]. See further the discussion in PG Turner, 'Rudiments of the Equitable Remedy of Compensation for Breach of Confidence' in Simone Degeling and Jason NE Varuhas (eds), *Equitable Compensation and Disgorgement of Profit* (Hart Publishing, 2017) 239, 260–1.
[145] For discussion of the doubts and confusion in this area, see Turner (n 144).
[146] *Giller v Procopets* (2008) 24 VR 1, [233], [418]–[419], [439] (Neave JA). See the discussion in Ibid 270–1.
[147] *Giller v Procopets* (2008) 24 VR 1, [233], [428] (Neave JA).
[148] (1990) 22 FCR 73, 87.
[149] Ibid 87. See similarly *Optus Networks Pty Ltd v Telstra Corporation Ltd* (2010) 265 ALR 281, [39].
[150] *Campbell v MGN Ltd* [2004] UKHL 22, [17] (Lord Nicholls).
[151] Michael Bryan, Vicki Vann and Susan Barkehall Thomas, *Equity and Trusts in Australia* (Cambridge University Press, 3rd ed, 2022) 194. Though Turner argues that equity should not provide compensation for harm to personal interests: Turner (n 144) 270–3.
[152] Bryan, Vann and Barkehall Thomas (n 151) 194.

First, then, to have 'the necessary quality of confidentiality', information must not be in the public domain or public knowledge.[153] Further, 'the nature of the information must be such that it is capable of being regarded as confidential',[154] as is the case for photographs relating to private activities that are taken surreptitiously, improperly or unlawfully.[155] As Gleeson CJ noted in *Lenah Game Meats*, though, it can be difficult to identify what is 'private':

> There is no bright line which can be drawn between what is private and what is not. … An activity is not private simply because it is not done in public. … Certain kinds of information about a person, such as information relating to health, personal relationships, or finances, may be easy to identify as private; as may certain kinds of activity, which a reasonable person, applying contemporary standards of morals and behaviour, would understand to be meant to be unobserved. The requirement that disclosure or observation of information or conduct would be highly offensive to a reasonable person of ordinary sensibilities is in many circumstances a useful practical test of what is private.[156]

In the employment context, employers gather and hold sensitive and personal information about their workforce, which might include, for example, employees' personal details, contact information, financial information, medical history, biometric data, and so on. This is likely to be 'private' information of a confidential character; in Gleeson CJ's terms, a reasonable person would likely see the disclosure of these types of information as being highly offensive. CCTV and surveillance data recorded in bathrooms, changing rooms and lactation rooms would also be likely to be seen as confidential, especially given – in some jurisdictions – it is likely to have been obtained unlawfully.[157] Data relating to an employee's location and movements outside of work hours, and during breaks, is also likely to be 'private' information of a confidential character in many contexts; a reasonable person, applying contemporary standards, would likely understand that our movements outside of work time are generally meant to be unobserved by an employer, and would find it highly offensive to be observed or tracked, or to have their location and activities recorded, when they are not on call or working.

More complex questions arise around other types of data, such as location data captured during work hours, keystroke and productivity data, and training history, for example, which, applying contemporary standards, are perhaps more likely to be expected to be observed and, therefore, unlikely to be private or confidential. That said, individual employees might not expect to be observed via keystroke monitoring software or CCTV, especially when such observation occurs without warning or notice, and particularly when that observation is directed to recording and monitoring an employee's physical ability or disability, which might be seen as something that is 'private'.[158] Further, while employers might monitor employee computer use and email correspondence, there may be personal material in that correspondence that a reasonable person would understand is meant to be unobserved, even if it is being accessed on a work device.[159] This might include personal correspondence, but also – for example –

---

[153] *Smith Kline & French Laboratories (Aust) Ltd v Secretary, Department of Community Services & Health* (1990) 22 FCR 73, 87; in the UK, see *Coco v A.N. Clark (Engineers) Ltd* [1969] RPC 41, 47; *Primary Group (UK) Ltd v The Royal Bank of Scotland Plc* [2014] EWHC 1082 (Ch) (11 April 2014) [209]; *Douglas v Hello! Ltd (No 3)* [2008] 1 AC 1, [122] (Lord Hoffmann); *Attorney-General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109, 268 (Lord Griffiths), 282 (Lord Goff).
[154] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 224 (Gleeson CJ).
[155] Ibid 224–225 (Gleeson CJ).
[156] Ibid 226 (Gleeson CJ).
[157] See, eg, the provisions in the *Surveillance Devices Act 1999* (Vic) Part 2A.
[158] See, eg, *Tilli v Fresh & Wild Ltd T/a Whole Market Foods* [2022] UKET 2204611/2019 (9 May 2022).
[159] cf *Madzikanda v Australian Information Commissioner* [2023] FCA 1445.

passwords to personal accounts, which a reasonable person would likely understand are meant to be unobserved.

The full scope of what is 'private' and 'confidential' in the employment context is therefore likely to be contested. That said, while some employee data in the workplace is unlikely to be seen as 'private', other types of information may well have 'the necessary quality of confidentiality'.

Second, for an equitable obligation to arise, confidential information must be communicated in circumstances importing an obligation of confidence.[160] As Megarry J expounded,

> It seems to me that if the circumstances are such that any reasonable man standing in the shoes of the recipient of the information would have realised that upon reasonable grounds the information was being given to him in confidence, then this should suffice to impose upon him the equitable obligation of confidence.[161]

This does not require the parties to be in a pre-existing or confidential relationship.[162] Further, the test is objective, not subjective.[163] The sensitive and personal nature of much information gathered in the employment context arguably makes it information that a reasonable employer should have known had a confidential character. This might apply to, for example, employees' personal details, contact information, location data (where captured outside of work hours), medical history, financial information, biometric data, and so on.

Third, there must be unauthorised use of the information.[164] Later cases have held that detriment may not need to be established.[165] Unauthorised use can be accidental or unintentional.[166] What is (un)authorised may be explicit or implicit, and may depend on how information is confided. In *Smith Kline*[167] the Full Court of the Federal Court of Australia considered the scope of the obligation imposed by the duty of confidence:

> Sometimes the obligation imposes no restriction on use of the information, as long as the confidee does not reveal it to third parties. In other circumstances, the confidee may not be entitled to use it except for some limited purpose. … there can be no breach of the equitable obligation unless the court concludes that a confidence reposed has been abused, that unconscientious use has been made of the information.[168]

In the UK case of *Primary Group (UK) Ltd v The Royal Bank of Scotland Plc* ('*Primary Group*'), the scope of the obligation was assessed 'from the perspective of the reasonable

---

[160] *Coco v A.N. Clark (Engineers) Ltd* [1969] RPC 41, 47; *Travel Counsellors Ltd v Trailfinders Ltd* [2021] EWCA Civ 38 (19 January 2021) [14].
[161] *Coco v A.N. Clark (Engineers) Ltd* [1969] RPC 41, 48 (Megarry J).
[162] *Primary Group (UK) Ltd v The Royal Bank of Scotland Plc* [2014] EWHC 1082 (Ch) (11 April 2014) [211]; *Campbell v MGN Ltd* [2004] UKHL 22, [14] (Lord Nicholls); *Attorney-General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109, 281 (Lord Goff).
[163] *Primary Group (UK) Ltd v The Royal Bank of Scotland Plc* [2014] EWHC 1082 (Ch) (11 April 2014) [211].
[164] *Coco v A.N. Clark (Engineers) Ltd* [1969] RPC 41, 48.
[165] See, eg, *Smith Kline & French Laboratories (Aust) Ltd v Secretary, Department of Community Services & Health* (1990) 22 FCR 73, 111–112; *Attorney-General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109, 281–2 (Lord Goff); *N.R.M.A. v Geeson* (2001) 40 ACSR 1, [58]; *NP Generations Pty Ltd v Feneley* (2001) 80 SASR 151, [21]. Indeed, Megarry J keeps this possibility open: *Coco v A.N. Clark (Engineers) Ltd* [1969] RPC 41, 48.
[166] Bryan, Vann and Barkehall Thomas (n 151) 198.
[167] (1991) 28 FCR 291.
[168] Ibid 303–304.

person standing in the position of the recipient of the information.'[169] The cornerstone is the equitable principle that the recipient of information received in confidence 'shall not take unfair advantage of it.'[170]

What uses are 'authorised', then, will differ based on context, and will hinge on whether an employer is (1) retaining the information itself (and, then, whether it can only be used for a limited purpose, and whether other uses are 'unauthorised'); or (2) revealing or disclosing the information to third parties.

In the first case, when an employer is retaining the information themselves, the question will be what use was 'authorised' and, conversely, what use might be unauthorised or 'unconscientious'. Depending on the facts, authorised use of employee data might include, for example, managing health and safety risks, enabling appraisal and performance management, and implementing administrative functions like payroll and getting in touch with emergency contacts or next of kin. It is likely to be authorised to use location data which relates to working hours to support performance processes, as to show that an employee was absent from work repeatedly without explanation.

Beyond these cases, though, there are a number of contemporary examples of employee data use that are likely to be unauthorised or 'unconscientious'. An employer using employee contact information to stalk an employee, send them unwanted personal messages,[171] or to approach them at their home address, is arguably unauthorised and unconscientious.[172] Using surveillance devices and CCTV to watch, harass or try to commence a personal relationship with an employee is also likely to be unauthorised.[173] Similarly, using personal passwords stored on a work device to access an employee's personal email account and personal cloud storage is likely to be unauthorised and unconscientious.[174] Use of employee data for new or different purposes (such as to build or train a new management algorithm) might also be unauthorised. Indeed, in *I-Admin (Singapore) Pte Ltd v Hong*,[175] downloading and possessing data, without consent, was held to be unauthorised use.[176]

The question, though, is how other documents – such as employment contracts, workplace policies, enterprise agreements or privacy consent forms – will influence how courts assess what is 'unauthorised' use, and the extent to which these instruments might make an otherwise 'unauthorised' use, authorised. In other words, if a certain use is envisaged by an employer's policy document, for example, and employees provide information in accordance with that policy, is that sufficient to make a use 'authorised'? It is likely that equity will focus on substance over form; meaningful, substantive consent (either explicit or implicit) to a

[169] [2014] EWHC 1082 (Ch) (11 April 2014) [237].
[170] *Seager v Copydex Ltd* [1967] 1 WLR 923, 931 (Lord Denning).
[171] Nicole Madigan, 'Woman Spied on by Her "Awkward" Boss in Sinister Stalking Case', *news.com.au* (online, 23 May 2021) <https://www.news.com.au/lifestyle/real-life/news-life/woman-spied-on-by-her-awkward-boss-in-sinister-stalking-case/news-story/3134247616933137c02db321b06d2043>. See also Australian Human Rights Commission, *Respect@Work: National Inquiry into Sexual Harassment in Australian Workplaces* (2020) 579 <https://www.humanrights.gov.au/our-work/sex-discrimination/publications/respectwork-sexual-harassment-national-inquiry-report-2020?mc_cid=1065707e3c&mc_eid=%5bUNIQID%5d>.
[172] And, where this is done by another employee in the course of their employment, the employer might be vicariously liable for their actions: see, eg, *Vestergaard Frandsen A/S v Bestnet Europe Ltd* [2013] UKSC 31, [27].
[173] Australian Human Rights Commission (n 171) 579.
[174] cf *Madzikanda v Australian Information Commissioner* [2023] FCA 1445.
[175] [2020] 1 SLR 1130.
[176] Ibid [66] (though that case related to a breach by a former employee, not the employer).

particularly use is likely required. So, for example, if employees provide confidential information in accordance with an employer's policy under threat of disciplinary action, this is unlikely to constitute 'consent' or authorisation of an otherwise unauthorised use.[177]

In the second case, where an employer is revealing or disclosing employee information to third parties, for some types of information, it may be that any disclosure to third parties is unauthorised, if prior employee consent has not been given. This might be the case for sensitive data, like medical information, out of hours location data, biometric data or disability status, for example. Sending employee data to third party platforms, where HR or payroll functions are outsourced, might then be unauthorised unless employees are notified and meaningfully consent to these data flows.[178]

Another unauthorised use of employee data might include the sale or distribution of employee data to third parties. This is highly likely to be unauthorised and, particularly where that data is monetised or commodified, unconscientious use of employee data. Another scenario might include data leaks, including those arising from a breach or hack of organisational systems, allowing third parties to access data. Again, this is likely to be unauthorised, and may be unconscientious if the employer's data systems are at fault.[179]

An equitable obligation of confidence might extend to third parties who receive employee data,[180] though the rules here are complex, and will turn on the facts of each case. In *Primary Group*, it was opined that if confidential information relating to A is disclosed by B to a third party, C,

> in circumstances where C knows, or ought to appreciate, that the disclosure is a breach of B's obligation of confidence to A … C will become subject to an equitable obligation of confidence owed to A. Accordingly, if C makes unauthorised use of the information, C will be liable to A for breach of confidence.[181]

However, if 'C believes, and a reasonable person standing in his shoes would also believe, that B is entitled to disclose the information to C for a particular purpose', then C 'will come under an equitable obligation to A only to use the information for that purpose.'[182] If the 'reasonable person in the position of C would make further inquiries … before making a particular use of the information' and C does not make those inquiries, C will also be liable for breach of confidence.[183] By contrast, if C has no actual knowledge that information is confidential or that it is being misused, and is not reckless to that fact, then they will generally not be liable for breach of confidence.[184] The conscience of a third party is not bound without notice.[185]

Some third parties might argue, then, that they had no knowledge that employee information is confidential, or that it is being misused by being transmitted to them. They might argue that it was reasonable to assume that employers are entitled to disclose employee data, for any

---

[177] cf *Construction, Forestry, Maritime, Mining and Energy Union v BHP Coal Pty Ltd* [2022] FWC 81.
[178] cf *Lee v Superior Wood Pty Ltd* [2019] FWCFB 2946.
[179] Though see the discussion below of *WM Morrison Supermarkets plc v Various Claimants* [2020] UKSC 12.
[180] *Attorney-General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109, 268 (Lord Griffiths).
[181] *Primary Group (UK) Ltd v The Royal Bank of Scotland Plc* [2014] EWHC 1082 (Ch) (11 April 2014) [238]–[240].
[182] Ibid.
[183] Ibid.
[184] *Vestergaard Frandsen A/S v Bestnet Europe Ltd* [2013] UKSC 31, [22], [26].
[185] Ibid [23].

purpose, to third parties; the data is therefore not being misused. This argument is likely to be more successful in Australia, with its limited privacy protection for employee data, than in the UK, especially since the expansion of data protection in the GDPR.

B. Overlapping and complementary protections

It is arguable, then, that a claim for breach of confidence might be raised to protect employee data. How, though, might statutory data regulation, common law and equitable rights overlap? Equitable obligations relating to confidential information may co-exist, in some circumstances, with contractual obligations.[186] In *Woodings v WA Glendinning & Associates Pty Ltd* ('*Woodings*'),[187] Smith J considered whether equitable breach of confidence could coexist with a contractual confidentiality provision, ultimately concluding that a contractual confidentiality provision does not inevitably oust equitable obligations of confidence[188] but, rather, the matter will turn on the effect and scope of the contractual provision,[189] and whether it creates 'equal or greater protection than the equitable duty of confidence'.[190] Endorsing Gordon J in *Coles Supermarkets Australia Pty Ltd v FKP Ltd* ('*Coles*'),[191] Smith J articulated 'the fundamental rule [as being] that equity will not intervene where there is an adequate remedy at law';[192] and this also applies to obligations of confidence.

By contrast, though, in *Streetscape Projects (Australia) Pty Ltd v City of Sydney* ('*Streetscape*')[193] the NSW Court of Appeal held that fiduciary obligations could not operate concurrently with contractual obligations, unless those contractual protections were inadequate.[194] In that case, though, the breach of confidence claim was remitted for re-trial, including to consider whether the information was confidential;[195] the Court's reasoning in relation to 'adequacy' was therefore not directly relevant to the breach of confidence claim. In *Streetscape*, too, the contractual obligations, fiduciary obligations and duty of confidence were pleaded as being 'co-extensive',[196] the claims in equity were framed to align 'precisely' with the terms of the contract[197] and to operate in 'parallel',[198] and the remedies awarded at first instance were the same across each ground of claim.[199] This perhaps makes the outcome and reasoning in *Streetscape* less surprising; if there is no apparent difference between the duties and their scope in contract and equity, then the role of equity might well be minimal, as contractual remedies are both adequate and equivalent to those in equity. *Streetscape*, *Woodings* and *Coles* therefore appear reconcilable in terms of their approach.

For Turner, though, the view in *Streetscape* is 'mistaken'.[200] Turner argues that equitable obligations are not conditional on the inadequacy of common law protections.[201] Instead, for

[186] *Optus Networks Pty Ltd v Telstra Corporation Ltd* (2010) 265 ALR 281, [29]–[30].
[187] [2019] WASC 54.
[188] Ibid [64].
[189] Ibid [68].
[190] Ibid [69].
[191] [2008] FCA 1915, [63]–[64].
[192] *Woodings v WA Glendinning & Associates Pty Ltd* [2019] WASC 54, [69].
[193] (2013) 85 NSWLR 196.
[194] Ibid 220 (Barrett JA).
[195] Ibid 228, 239 (Barrett JA).
[196] Ibid 214 (Barrett JA).
[197] Ibid 214 (Barrett JA).
[198] Ibid 219 (Barrett JA).
[199] Ibid 219 (Barrett JA).
[200] Turner (n 144) 252.
[201] Ibid.

Turner, a contract might provide evidence that a party consented to forsake any equitable obligation of confidence; forsaking the benefit by consent – which might be, but need not be, evidenced by a contract – is the reason contractual and equitable obligations might not co-exist.[202] Turner's view, then, is that 'concurrent obligations of confidence can exist in contract and equity except where a contrary intention is shown.'[203]

In the Australian employment context, though, this might be further complicated by the High Court's decisions in *Commonwealth Bank of Australia v Barker*,[204] *Construction, Forestry, Maritime, Mining and Energy Union v Personnel Contracting Pty Ltd*[205] and *ZG Operations Australia Pty Ltd v Jamsek*[206] which emphasise the primacy of the written employment contract in Australian law. Following this approach, Australian courts may be reluctant to develop equitable principles where an employment contract is in place, particularly if that development is seen as 'beyond the legitimate law-making function of the courts'.[207]

That said, courts may view the incremental development of established equitable principles – which does not involve the creation of a new normative standard[208] – differently to the development of implied terms, or the creation of (arguably) new principles of contractual interpretation. Further, while many employment contracts include terms relating to the *employee's* obligations of confidentiality,[209] it is rarer to impose contractual responsibilities of confidentiality on *employers*. This may be an area, then, where contractual obligations are absent, or inadequate, for protecting employee data. Unlike in *Streetscape*, employment contracts may well '[provide] little by way of safeguards for' employees.[210]

The potential and limits of equitable breach of confidence, and its complementarity to other statutory and common law protections, is aptly demonstrated by the UK Supreme Court case of *WM Morrison Supermarkets plc v Various Claimants* ('*Morrisons*').[211] In that case, the Supreme Court considered whether an employer was vicariously liable for a data breach effected by an employee. The employee maliciously copied and leaked payroll data of 98,998 Morrisons employees. At trial, Langstaff J held that Morrisons had no primary liability, but were vicariously liable for the employee's actions, including for breach of statutory duty under the DPA, misuse of private information, and breach of the equitable duty of confidence.[212]

The Supreme Court held, in *obiter*, that vicarious liability applies to breaches of the DPA, and for the breach of obligations at common law or in equity, 'committed by an employee who is a data controller in the course of his employment.'[213] However, in this case, the acts could not 'fairly and properly be regarded as done by him while acting in the ordinary course of his employment',[214] meaning there was no vicarious liability.

---

[202] Ibid 253.
[203] Ibid 255.
[204] (2014) 253 CLR 169.
[205] (2022) 275 CLR 165.
[206] (2022) 275 CLR 254.
[207] *Commonwealth Bank of Australia v Barker* (2014) 253 CLR 169, 178, 195 (French CJ, Bell and Keane JJ).
[208] cf ibid 185 (French CJ, Bell and Keane JJ).
[209] The ABS Short Survey of Employment Conditions found that non-disclosure clauses were used by 45.3% of Australian businesses in 2023: Australian Bureau of Statistics, 'Restraint Clauses, Australia, 2023', *ABS*, 21 February 2024 <https://www.abs.gov.au/articles/restraint-clauses-australia-2023>.
[210] *Streetscape Projects (Australia) Pty Ltd v City of Sydney* (2013) 85 NSWLR 196, 219 (Barrett JA).
[211] [2020] UKSC 12.
[212] Ibid [11].
[213] Ibid [55].
[214] Ibid [47].

The claimants in *Morrisons* also made an equitable claim for breach of confidence, seeking both primary and vicarious liability. In their pleadings, the claimants sought an injunction to prevent Morrisons further disclosing the private and confidential information; this was not pursued at trial.[215] The High Court held that Morrisons had no direct liability under the DPA, as it was not the data controller at the time of the breach;[216] the DPA did not create absolute or strict liability.[217] Similarly, there was no direct liability for breach of confidence or misuse of private information; 'it was not Morrisons that disclosed the information or misused it'.[218] It appears, then, that the release of private employee data – via a malicious employee data leak – is unlikely to lead to primary liability for breach of confidence for employers. In other cases of unauthorised use, though, employee data might well be protected by equity.

C. Strengthening employee data protection

The benefits of bringing a claim for breach of confidence are clear in Australia, where there is limited statutory or constitutional regulation of privacy and data protection in the workplace. Equity might offer a path to protect employee data, in the absence of other legal protections. It also offers three specific advantages over and above protections traditionally provided by labour law.

First, it is possible to argue that equitable obligations extend to those who are no longer, or not yet, in an employment relationship.[219] This is far broader in scope than the obligations under employment contract law, which only extend to the contractual parties, and often only for the duration of the contract. So information and data gathered during recruitment processes, or held at the end of the employment relationship, might be protected. This is particularly significant given employers in Australia are generally under no obligation to destroy employee records at the end of the employment relationship, or after a certain period of time; or to ensure employee records (or former employee records) are up-to-date or accurate.

Second, it may be possible to seek remedies in equity against third parties that receive employee data who are not party to the employment relationship,[220] though this will turn on the facts of each case. The significant data flows to third parties in *Lee* illustrate the potential practical relevance of this aspect of equitable obligations. It is also not necessary to show that employees have proprietary rights in their information or data to seek an equitable remedy. With the fissuring of the employment relationship,[221] and the growth in the number of entities involved in the workplace, equitable protections could have growing significance over time.

Third, equity is unconcerned with employment status, or the formal categorisation of the relationship between the parties, so long as information is imparted in 'confidence'. This means there is scope to ensure protection of data for those who are not classed as 'employees', or even

[215] *Various Claimants v WM Morrison Supermarkets plc* [2019] QB 772, [10].
[216] Ibid [50].
[217] Ibid [62].
[218] Ibid [65].
[219] See, eg, *Travel Counsellors Ltd v Trailfinders Ltd* [2021] EWCA Civ 38 (19 January 2021); *Trailfinders Ltd v Travel Counsellors Ltd and Ors* [2020] EWHC 591 (12 March 2020).
[220] *Attorney-General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109, 268 (Lord Griffiths).
[221] David Weil, *The Fissured Workplace: Why Work Became So Bad for So Many and What Can Be Done to Improve It* (Harvard University Press, 2014) ('*The Fissured Workplace*').

'workers'.[222] This offers significant advantages over the limited scope of labour law, which is typically confined to 'employees'. As Stewart and others have argued, the High Court's decisions in *Construction, Forestry, Maritime, Mining and Energy Union v Personnel Contracting Pty Ltd*[223] and *ZG Operations Australia Pty Ltd v Jamsek*[224] – emphasising the primacy of the employment contract over the primacy of fact in establishing employment status where agreements are wholly in writing – have potentially endorsed and encouraged the use of contractual drafting and superior bargaining power to present workers as 'contractors', not employees.[225] Equity, though, is focused on substance not form; it could offer significant benefits to those excluded from employment protections.

In jurisdictions like the UK, with rigorous data protection laws, an action for equitable breach of confidence might still offer benefits, even if the ultimate outcome in *Morrisons* was the same, under statutory privacy law, common law and equity. Key to this lies in the remedies available. Equitable remedies are wide ranging and flexible; this may prove superior to other remedies available in other areas of law. For example, an account of profits might be a particularly relevant remedy in this context, and one only available in equity in Australia.[226] The benefit of pursuing such a claim is therefore particularly clear when – as in Australia – statutory privacy law is enfeebled; but it may also offer benefits in other jurisdictions, with more developed regulatory provisions.

V. CONCLUSION: NEW FRONTIERS, AUSTRALIA?

It remains to be seen whether statutory reform addresses the privacy and data protection gaps in the employment context in Australia. If change is pursued, the UK offers one example of how Australia could develop its legislative framework in this area. Critical to this, though, is better articulating what is 'private' in the employment context. Employers clearly have an interest in collecting data on employee performance and productivity. In some cases, collecting sensitive and personal information – like health records – might be critical for meeting legislative health and safety obligations, for example. That said, employees do not renounce all rights to privacy in the employment context: the art 8 case law prompts us to recognise that employees might maintain a right to 'private life' and correspondence, even when at work; this could limit the scope of workplace monitoring and surveillance. Further, even if it is necessary and reasonable for employers to collect private and sensitive data from employees to fulfill some functions, there should be limits on how that data is used, kept, and further distributed.

In the absence of legislative reform, courts and advocates could look to equity to better protect employees' data and personal information. While tort offers another potential route,[227] the incremental development of equitable principles should be considered as a potential avenue for developing protection of privacy.[228] Australian case law demonstrates a cautious approach to legal development, which might confine the scope for equitable principles to be developed in this way. That said, equity can and should strengthen the employment contract in an era of

[222] See, eg, *Construction, Forestry, Maritime, Mining and Energy Union v Personnel Contracting Pty Ltd* (2022) 275 CLR 165; *Uber BV v Aslam* [2021] UKSC 5.
[223] (2022) 275 CLR 165.
[224] (2022) 275 CLR 254.
[225] Andrew Stewart, Mark Irving KC and Pauline Bomball, 'Shifting and Ignoring the Balance of Power: The High Court's New Rules for Determining Employment Status' (2023) 46(4) *UNSW Law Journal* 1214, 1245.
[226] *Hospitality Group Pty Ltd v Australian Rugby Union Ltd* (2001) 110 FCR 157; cf *Attorney-General v Blake* [2001] AC 268.
[227] Indeed, Turner argues this would be the more congruent route to protect personal interests: Turner (n 144) 272.
[228] See, eg, *Smethurst v Commissioner of Police (Cth)* (2020) 272 CLR 177, 273 (Edelman J).

mass surveillance and data gathering. Given the law in Australia is otherwise inadequate to protect employee privacy rights, equity can and should step in.[229] If legislative reform occurs, equity could offer complementary protection for employee privacy rights, as the situation in the UK illustrates. As employer data gathering and workplace surveillance continue to gain pace, this is an area that requires multiple forms of legal intervention, to ensure employees have meaningful rights to privacy at work.

[229] On equity's role, see, eg, *Wolverhampton City Council v London Gypsies and Travellers* [2023] UKSC 47, [238] (Lord Reed, Lord Briggs and Lord Kitchin (with whom Lord Hodge and Lord Lloyd-Jones agree).