



Workplace biometrics: Protecting employee privacy one fingerprint at a time

journals.sagepub.com/home/eid



Peter Holland 

Swinburne Business School, Swinburne University of Technology, Australia

Tse Leng Tham 

RMIT University, Australia

Abstract

This article examines the contested terrain of protecting or providing biometric data in the workplace. Through a major case study in Australia, a decision to terminate employment on the grounds of non-consent for biometric data to be collected was overturned through the legislative system. The case is important in that it highlights the increased impetus to collect such data and the arbitrary nature of legal protection. However, the results of this significant case do provide improved clarity and guidance on the usage, collection, storage and management of biometric data. It also signals to management the need to understand employees' rights and their own obligations around the informational privacy of employees.

Keywords

Biometrics, data security, employee consent, fingerprints, privacy

Introduction

Whilst monitoring and surveillance has been a fundamental aspect of the employee relationship for centuries, work has evolved and along with it, ever more sophisticated ways have been developed to monitor and observe the workforce. In recent times, such developments are due largely to the advance of information technology and communications (ICT) which have created a profound shift in not just the way work is carried out, but the extent to which monitoring and surveillance has evolved especially in the first two

Corresponding author:

Peter Holland, Swinburne Business School, Swinburne University of Technology, BA Building, Hawthorn, Victoria 3122, Australia.

Email: pjholland@swin.edu.au

decades of the 21st century (Allen et al., 2007; Barnes et al., 2018; Lane, 2003). An emerging example of this is the increased opportunity to collect and use biometric information in the workplace. This has emerged in an environment where there is a considerable lack of understanding as to the significance of collecting such data by both management and employees, and a certain degree of legal uncertainty and ambiguity regarding employee rights to the protection and privacy of their data (Ball, 2010; Barnes et al., 2018; Holland et al., 2015). This article examines the ongoing tensions between the rights of management to collect such data and to sanction employees who refuse, and an employee's right to privacy. In doing so, this study provides a new understanding of the contested issues around the collection, storage and use of biometric data, protection and privacy through the lens of the Australian workplace and important insights for the broader human resource management and employee relations community.

Biometrics and the workplace

Biometrics typically refer to technologies that are used to measure and analyse unique characteristics of an individual which are generally considered innate, immutable and distinctive to that individual (Du et al., 2011; Magnet, 2011; Moradoff, 2010). Typically, these fall into two categories: physiological, which can include blood type, fingerprints and hand geometry; and physical and behavioural, for example, a person's gait, voice patterns or facial identification (Jackson, 2009; Norris-Jones, 2012). Biometric recognition technologies are becoming a common feature of the workplace with iris, facial or fingerprint scanners replacing the conventional text-based passwords, swipe-cards and pin numbers. Biometrics are seen as a reliable option for identity authentication and/or verification for the purposes of workplace security, access control, theft prevention and attendance record-keeping (Carpenter et al., 2016). It is argued that they are more accurate and convenient and as noted, physiological and behavioural aspects are unique to that individual and are not easily replicable (Ball, 2010; Jackson, 2009; Nanavati et al., 2002; Rao, 2018; Zielinski, 2018). An additional factor to security is cost, as biometrics log-on authentication reduces time costs by replacing the conventional password authentication method where passwords can be lost or forgotten and are

required to be changed and can tie up help desks in rebooting systems where these passwords are forgotten. All this can be replaced with a single fingerprint sign-on system. This significantly reduces time to log on and the problems when such inputs are forgotten by users (Aponovich, 2001). As these features are unique, they do not need updating or resetting and importantly, they cannot be lost! Biometric recording of employee time and attendance has also been purported to be a more reliable and accurate means of ascertaining an employee's hours worked (Rao, 2018; Zielinski, 2018), and more effective in preventing 'buddy punching', where employees clock in and out for friends who may not have been physically present for work (Hussain, 2015).

Despite such apparent benefits of the use of biometric technology at the workplace, its introduction has spurred considerable debate and even resistance in its adoption (Rao, 2018). Carpenter et al.'s (2016) review of the literature suggests that some of these key concerns include: (1) the creation of a pervasive and omnipresent regime of surveillance technology where perceived bodily privacy is being infringed, especially where the scope of monitoring is not clearly defined (Ball, 2010; Bolle et al., 2004); (2) the extent to which such biometric data will be used for the intended purposes only; and (3) the security of data storage (Rao, 2018). The first two issues run together. Biometrics information is highly personal and can potentially reveal private details of an individual, particulars that even the individual may not have knowledge of. By extension, this may risk providing additional information without the overt consent of the employee (Ball, 2010). For instance, fingerprint data can reveal, with up to 90% accuracy, an individual's gender and could potentially detect genetic disorders (Dantcheva et al., 2015; Zhai and Qui, 2010). This opens up potential fears of, and possibilities for, systematic discrimination should such information be intentionally or unintentionally taken into account to make decisions related to recruitment, promotions and conditions of employment (Currah and Mulqueen, 2011). Indeed, such concerns have already been raised in the US with regard to discrimination against consumers in the data broker industry, where consumers are assigned marketing 'scores' and classified into categories based on race, ethnicity and income levels (Schneider, 2015). For instance, Stewart (2019) raises concerns over discrimination in instances where businesses may target lower scoring categories (i.e. of certain race and/or income levels) with marketing efforts of subprime credit, provision of subpar service levels or denial of access to insurance applications. Additionally, this also puts into question whether certain personal boundaries are being crossed without the knowledge and consent of the employee. With the collection of biometric data such as facial geometry and gait, it is theoretically possible to re-identify an anonymous individual even in publicly accessible areas. This essentially creates the possibility of omnipresent surveillance (Schumann and Monari, 2014). Indeed, as Barbeler (2018) points out, the ethical question then arises as to how reasonable it is for employers to require employees to provide biometric data. Moreover, studies have indicated that when such organisational monitoring or surveillance extends beyond the realm of work-related performance, employees often see such policies to be an invasion of privacy (Alder and Ambrose, 2005) and signs of mistrust (Holland et al., 2016). Employees are more likely to adopt defensive measures as a response, including unionisation (York and Carty, 2006) or renegotiation of labour contracts (Kelly and Herbert, 2004).

The third key concern suggested by Carpenter et al.'s (2016) review of the collection and use of biometric data in the workplace revolves around data security and safety (Rao, 2018). The issue of privacy and safety of these unique data in an era of highly sophisticated 'hacking' raises an obvious concern. Essentially, biometric data such as fingerprint patterns are scanned and recorded in digital form and therefore can be hacked and easily 'stolen' (Roberg-Perez, 2017). Furthermore, fingerprints can be 'lifted' from coffee cups or keyboards. As such, the notion of the increased level of security from such biometric data needs to be considered in the context of how it can be compromised and how, from a human resource management perspective, it can compromise the employment relationship.

Employee privacy in the digital era

The digitisation of the workplace has generated considerable debate over the concept of privacy for the employee (Determann and Sprague, 2011; Sewell and Barker, 2006; Stratton and Stam, 2003). Whilst the concept of privacy can be elusive as it can be seen as a multi-dimensional construct which has variance in its interpretation in different legal jurisdictions (Ball et al., 2012), it is worth exploring the seminal work on contemporary privacy as a foundation for understanding its position in the (electronic) workplace.

The main contemporary theories of privacy were developed by Westin (1967) and Altman (1975). As Margulis (2003) notes, their theories on privacy are both insightful and have stood the test of time. Westin (1967) identified the fact that privacy operates through individual, group, organisational and institutional levels, propounding that the individual proactively manages their privacy, and that tensions arise from intrusions into previously balanced relations between the public and private self which were not anticipated. The key intrusive force he identified as technology. Although written over 50 years ago, this argument is probably more relevant today than ever before. In an imbalanced state, Westin argues that people are less protected than before in terms of their privacy and potentially their data against the intrusion. Not least, in Westin's framework of privacy, was that the individual could limit and protect their information and communications by setting boundaries for sharing information with trusted others (Margulis, 2003; Westin, 1967). However, this concept can effectively be undermined by the depth and extent of electronic monitoring and surveillance supported by advanced ICTs whether planned or unplanned. The later work of Altman (1975) built on these integrated aspects of privacy but crucially focused on the dynamic and changing nature of the environment within which privacy operates, i.e. the context (Altman, 1975, 1990; Margulis, 2003). Whilst Altman's approach (as that of Westin's) identified the perceived control the individual had over their privacy, Altman also noted that privacy was bi-directional, involving input from others to create this privacy. This final point was further developed by Petronio (2002), through the theory of Communication Privacy Management (CPM). This theory explores the tension or turbulence at and around setting the boundaries of monitoring and surveillance and the permeability or impermeability of these borders. Subsequent research by Stratton and Stam (2003), in the context of contemporary ICT, identified CPM as a constructive framework to explain this contested terrain. Nevertheless, research by Allen et al. (2007), looking at this theory in the context

of electronic monitoring and surveillance (EMS), found that the model needed modification to account for the new and more invasive aspects that EMS creates in the employment relationship. Such shortfalls of CPM theory in explaining contemporary forms of monitoring or surveillance are thrown into sharper relief given the unique characteristics of biometrics data as discussed in preceding sections in this article. This is an important point, because whilst CPM emerged at the start of the 21st century, the exponential changes we have seen in the following two decades including smart devices and social media, as well the cost reduction and availability, make contemporary (such as biometric) and electronic forms of monitoring and surveillance far broader, more intense and invasive (Chang et al., 2015). However, whilst deficiencies in these theories have been identified, what they do provide is the opportunity to reflect on and frame how privacy in the contemporary workplace can and should be managed by the individual employee and others (e.g. employer) – particularly in an era where digital and other forms of surveillance technologies increasingly encroach on the rights and expectations of the workforce. As Petronio et al. (1998) argue, individuals have a need for and expectation of privacy. In the workplace, there need to be boundaries on how much of oneself is revealed to the employer (Fairweather, 1999), especially in this era of intense and relentless electronic monitoring and surveillance both inside and outside the workplace.

The need for legal boundaries and guidance in these emerging employment issues is critical in building robust and fair policies to provide checks and balances within a system and to build trust in the management of these issues in the workplace as technological changes and advancements move apace (Holland et al., 2015). As Sewell and Barker (2006) have argued, the introduction of contemporary and electronic forms of monitoring and surveillance can be framed as coercive or caring and is not often done in a cooperative approach with the workforce (Allen et al., 2007). In this context of organisation-driven boundaries on privacy, Allen et al. (2007) and Sewell and Barker (2006) note, most employees want to be seen as good employees and as such do not want to challenge the organisational strategies. As Petronio (2002) also argues, employees effectively exchange privacy for employment. As such they may lack the power, motivation and significantly the knowledge to understand the legitimacy of EMS and therefore the need to limit boundary ‘creep’ around privacy issues (Ball et al., 2012; Mason et al., 2002). However, legal provisions around the world mostly rely on personal data protection and privacy legislation (Hugl, 2013). For example, in the EU, where data privacy laws define biometric data as a special category of personal data, the General Data Protection Regulation (GDPR) endeavours to address these issues and provides a uniform framework across the EU including the UK, although there are variations within EU countries (Hugl, 2013). Similarly, the need for a unique legal framework concerning the collection, storage and management of biometric data has also been recognised in the United States, firstly by the state of Illinois with the Illinois Biometric Information Privacy Act (BIPA) in 2008 (Krishan and Mostafavi, 2018). BIPA has been heralded as one of the strictest biometric privacy laws to date, governing the collection, use and storage of biometric data, and above all, it permits individuals harmed by BIPA violations to take private action for damages (Krishan and Mostafavi, 2018). However, it is important to note that such a legal framework is missing from the US at a federal level

and only three states (Illinois, Texas and Washington) have enacted legal frameworks in regard to the collection, use and management of biometric data (Gemalto, 2019). Concerns surrounding conflicting definitions and standards of regulation among these different statutes have been raised and the concerns simultaneously highlight the complexities associated with the management and protection of such sensitive data (Krishan and Mostafavi, 2018; Stewart, 2019).

In an Australian context, the following case study highlights these ongoing tensions. The case focuses on the biometric data associated with fingerprints. It also provides a test and framework for legal and management consideration of the boundaries of privacy and managerial prerogative regarding the provision and protection of biodata in the workplace.

Biometrics in the Australian workplace

Like many advanced market economies (AMEs), the Australian workplace has increasingly been permeated by ICTs, often seamlessly. However, with regard to the issue of biometric data, tensions can be traced back over 15 years to the first case to test the validity of such a system for time management and attendance records. In 2002, Qantas proposed a biometric-based time and attendance system using fingerprint scanning. In the first instance, the Transport Workers' Union of Australia (TWU) raised concerns regarding the protection of these data, which they took to the trade union umbrella body, the Australian Council of Trade Unions (ACTU). The ensuing dispute was taken to the Australian Industrial Relations Commission; however, further negotiation between the TWU and Qantas saw the dispute settled outside court. Qantas agreed not to proceed with the biometric time management and attendance system and instead introduced an electronic swipe-card, reflecting the perceived negative impact such a system would have on the employment relationship (see Alder and Ambrose, 2005; Holland et al., 2016; Martin et al., 2016). The tensions biometric systems created were summed up in a statement from the then national secretary of the TWU, John Allan, who stated his members remained concerned about the fingerprinting system as they saw it as akin to being treated like suspected criminals. As such, his members found the technology insulting and that meetings with the manufacturer of the system failed to assuage their concerns (WPX, 2003). Since this period, as noted, the reduced costs of this technology have made it increasingly available to a wider cross-section of organisations outside of large corporations. It is in this context that the most significant test case on biometric data use and protection emerged. We explore this case study of *Jeremy Lee v. Superior Wood Pty Ltd* in Australia further in the following sections.

Case study: *Jeremy Lee v. Superior Wood Pty Ltd*

Background

Superior Wood Pty Ltd operates two saw-mills in the southeast of the state of Queensland. As a way to increase the efficiency of its human resource attendance systems, the company announced in early 2017 that it was introducing a biometric

(fingerprint) scanner. Mr Lee objected on the grounds that he was concerned about the collection and safe storage of his personal biometric information by the company. Unable to resolve the issue, in February 2018 Mr Lee was issued a letter of termination of employment on the grounds that he refused to adhere to the company's attendance policy. Through the national employment relations legal framework, the Fair Work Commission, a hearing was undertaken, citing that the dismissal was harsh, unjust or unreasonable, but Mr Lee was subsequently unsuccessful in having his termination overturned. The commissioner ruled that Mr Lee failed to follow the lawful and reasonable attendance policy. Mr Lee argued that the Privacy Act was also breached by this decision and was granted leave to appeal the decision as this case was seen to raise 'important, novel and emerging issues' in the workplace.

The case

In early 2017, when Superior Wood Pty Ltd announced its intention to introduce a biometric finger scanner to streamline its attendance and record-keeping, Mr Lee expressed his concerns at providing his biometric data to the organisation. During the trial period of the biometric scanner, from November 2017 to February 2018, Mr Lee had several meetings with management who sought to allay his fears regarding protection and privacy of his personal data. Mr Lee continued to refuse to provide his biometric data as his concerns were not addressed to his satisfaction regarding rights to protect his data and informational privacy. The issue was subsequently escalated to a first and then a final warning as the trial period came to an end and the biometric system was fully adopted. During this period, Mr Lee continued to sign in on the attendance log at the entrance. On 18 February 2018, Mr Lee was issued a termination notice, as the only employee of 400 who had refused to provide his biometric data and therefore not use the biometric employee attendance system.

The dispute went to the Australian Fair Work Commission in November 2018, as the first case challenging and seeking remedy to the requirement (and refusal) to provide biometric data, on the grounds the dismissal was unfair. During the case, management argued that whilst the focus was on attendance, this new system provided a higher level of health and safety information in a dangerous environment. Management (Mr Finlayson) acknowledged that Superior Wood Pty Ltd did not have a privacy policy reflecting the principles of the Privacy Act 1988, which governs employee privacy rights, or a confidentiality policy. In addition, Mr Finlayson on behalf of management, acknowledged that no notice letter had been sent to employees regarding the storage of data by a third party and that the biometric information was held by an independent party offsite.

The Fair Work Commissioner found that, firstly, the site attendance policy was neither unjust nor unreasonable on the grounds of improving the integrity and efficacy of the payroll systems and safety. Thus, non-compliance with the policy with adequate precautions would not render the policy invalid. Of more significance to the general use of biometrics at work was that despite concerns regarding the process of information management, particularly the use and storage of the data, raised by the employee, on balance the Commissioner was satisfied that the third-party holder of the data understood

their obligations under the Privacy Act. The Commissioner also found the collection of biometric information by management to be reasonable and necessary to carry out its activities. She was also swayed by the fact that only one person (Mr Lee) out of 400 dissented to the biometrics scanning. This finding also took into account that Mr Lee did suggest alternate remedies and Superior Wood failed to inform him of his rights under the Privacy Act or undertake any effort to seek an alternate remedy. Therefore, as Mr Lee failed to follow site attendance policy, the Commissioner deemed the termination of employment was neither harsh, unjust nor unreasonable. An appeal was lodged in January 2019, on the grounds that this was a unique case of interest in the context of the wider workplace impact and on the employment relationship. The case was subsequently heard by the Full Bench of the Fair Work Commission in May 2019.

The appeal focused on the ownership and protection of the appellant's biometric data under the Privacy Act 1988. In this case, Mr Lee's refusal to provide these data was not a valid reason for dismissal, on the premise that this change in policy was not part of the original employment contract – the Full Bench was satisfied that this was the case. In addition, the Full Bench found that Superior Wood Pty Ltd breached the Privacy Act by not providing the appropriate information regarding the use and storage of employees' biometric data and management regarding the collection and control of the data, and could not apply for employee records exemption as no information was provided. In addition, the Full Bench noted that providing consent under the threat of discipline or dismissal is not genuine consent. As such, Mr Lee's refusal to comply with the biometric attendance policy was not deemed a valid reason for dismissal. Therefore, the dismissal was found to be unjust.

Discussion

This case raises a number of issues and concerns from a human resource management and an employee relations perspective. As per CPM theory, this case also highlights the tension and turbulence at and around the setting of boundaries of monitoring and surveillance and the permeability or impermeability of these borders. Obviously, the issue of privacy is front and centre in the discussion, but we will return to this point. Taking a chronological view of the development of the case provides significant insights into several major issues. Firstly, whilst the introduction of the biometric HR system at Superior Wood Pty Ltd was announced as a *fait accompli*, this in normal circumstances in itself is not illegal; it is the first change in the boundaries of privacy around biometrics. However, with regard to gathering sensitive information such as biometric data, this falls under the Privacy Act where strict policy guidance is required, to prevent unauthorised breaches. We would also argue that the procedures in which Superior Wood Pty Ltd engaged through the introduction and enforcement of the biometric system of attendance recording reflect a poor management style which lacked consultation and discussion (Sewell and Barker, 2006). Secondly, in relation to management's legal obligation to protect employee data, the lack of due process in the form of providing information to employees regarding the gathering of their data and protocols for management and storage (including a privacy policy) of the data made the collection of data unlawful under the Privacy Act. Although it is worth noting that had Mr Lee initially agreed to the

taking of his biometric data and then dissented, he would not be covered under this Act, rather employee records exemption provisions which would not have allowed him the right to challenge the initial judgement. This focuses on the fluidity and permeability CPM theory highlights regarding the boundaries of biometric monitoring and surveillance in Australia. Although the Commissioner in the first case found the issue of lack of information to employees regarding their informational privacy to allow them to inform their decision to be disturbing, this was not deemed significant or acceptable permeability to overturn the dismissal. However, what was of concern was that in legitimately raising issues of information privacy and protection, the employee was subject to a series of disciplinary measures, or as Sewell and Barker (2006) highlight, coercion in the implementation of the system, culminating in his eventual dismissal, despite Mr Lee showing a willingness to comply with the attendance being recorded by alternative means that were never explored by management. It also had the potential to send a message to the rest of the workforce, regarding the consequences of challenging management's prerogative. In this context, it was of equal relevance that the Commissioner in the original case noted that in referring to the test case of *Woolworths (t/as Safeway) v. Brown (Woolworths)* on attendance, she found that the site attendance policy was not unjust or unreasonable.

The Commissioner made the point in the context of the Woolworths case that it is reasonable for an employer to improve safety and administration procedures (including cost reductions). This right for the business to manage its affairs by default increases the permeability of the privacy boundaries of the workplace. This was done in the current case at the expense of, and in breach of employees' personal and unique biometric data for a mundane policy of payroll and attendance management. It is interesting to note that in Austria, for example, such attendance systems requiring biometric data are subject to judicial approval (Hugl, 2013). Under the Illinois Biometric Privacy Act, employers are required by law to have a written policy detailing how employees' biometric data will be collected, used, stored and disposed of (Krishan and Mostafavi, 2018). Equally, swipecards or other devices could be argued to have been as effective without the potential of compromising personal information and potentially the informational privacy of the whole workforce. These were also points raised by Mr Lee. However, in response to these suggested alternatives, the Commissioner stated that these would have increased inefficiencies (costs) in the system and would have been an onerous burden on the company. As noted, considering the implications of increasing permeability of the privacy (biometric) boundaries of the workplace it is indeed a point of considerable debate.

In addition, the Commissioner stated that all the other employees had given implied consent to the collection of their personal data by registering their data with the company (without any information or consultation). However, as noted in the case, the fact remains that these employees were giving consent without the barest of facts or the required due process regarding the information they should have been given to provide at least a perception of informed consent about the process and the legal boundaries they were entitled to regarding the handing over of such sensitive personalised data. These issues reflect the points made by both Allen et al. (2007) and Sewell and Barker (2006) that most employees want to be perceived as good employees and as such do not want to

challenge their organisation's policies, processes or boundaries. It also highlights the point made earlier regarding the reduced cost of such technologies making them available to organisations with fewer resources or structures (i.e. a HR department), skills or knowledge to manage these boundaries noted in CPM theory, or the impact of these work patterns and policies. In the context of the coercive and punitive approach the management took to Mr Lee's attempts to seek an alternative solution, Petronio's (2002) point that employees effectively exchange privacy for employment is put into sharp relief in this case. It is through management actions that employees can clearly be seen to lack the perceived power, motivation or significantly the knowledge to understand and address the legitimacy of the taking of biometric data or the privacy implications, and therefore to defend or push back against such challenges (Ball et al., 2012; Mason et al., 2002). The fact, as it was revealed, that the data were held on multiple sites by a third party and potentially accessed by multiple people without the knowledge of the workers, was ameliorated by the original Commissioner's position that the IT organisation charged with the management of the data knew its obligations in securing data. Considering this act of faith was provided by a legal expert is in and of itself an interesting point rather than focusing on the lack of due process. The fact however remains that the request for biometric data was unlawful under the Privacy Act, but Mr Lee's refusal to provide his biometric data under any circumstance overrode Superior Wood Pty Ltd's breach in the eyes of the original Commissioner. In fact, Mr Lee provided evidence of alternate approaches, indicating his willingness to comply with the attendance policy – just not to provide his biodata. On this, Superior Wood Pty Ltd failed to investigate these alternatives provided by Mr Lee. Despite this again being clearly a coercive act on behalf of the management towards Mr Lee, the Commissioner accepted that there were alternative solutions but indicated that they were not as effective at capturing biodata or as helpful in quickly identifying who was on site. Indeed, in this respect the situation may be described as a caring framing of the decision to implement the biometric system (Sewell and Barker, 2006). It is worth again noting that the focus here is on simple attendance records. The Commissioner, therefore, supported the introduction of the biometric scanners and subsequently upheld the dismissal of Mr Lee as being reasonable for his refusal to provide his biodata – an act which was in breach of the site attendance policy in November 2018.

The appeal was granted in January 2019, on the important grounds that this was the first time the Full Bench of the Australian Fair Work Commission had considered the question of the refusal of an individual to provide biometric data to their employer. As such, the appeal raised important novel, and also emerging issues which are in the public interest. The key findings in this appeal were centred on the fact that these were new contractual procedures which were not strictly agreed to by Mr Lee and were not part of his original employment contract. As such, the focus turned to how reasonable and lawful the direction to use the biometric scanner was. The Full Bench of the Fair Work Commission found that in directing Mr Lee to submit to the collection of his biometric data in the form of a fingerprint, where he did not consent, was not a lawful direction by the organisation. Further, the Full Bench noted that any consent forthcoming after the threat of discipline and dismissal was not likely to be consent given freely, reinforcing Sewell and Barker's (2006) argument that these policies are often undertaken in a

coercive manner. In the context of CPM theory, changing the original boundaries around the capture of biometrics resulted in the organisation's direction to be deemed unreasonable and that Mr Lee's refusal to comply with the new attendance policy was not regarded as a valid reason for dismissal. In reviewing the case further, the Full Bench stated they believed that the Commissioner was in error when taking into account the purpose of the policy: improving the payroll system and what Sewell and Barker (2006) note as the perceived caring approach of the potential for improving health and safety checks in relation to the cost of alternative processes. In this current case, the management of Superior Wood Pty Ltd deemed that the improvements to the payroll system took precedence over the Privacy Act. Ultimately, the Full Bench concluded that Superior Wood Pty Ltd's breaches included a lack of information provided to employees on the collection, storage, protection and management of their biometric data as required by the Privacy Act. Additionally, what was overlooked here was also Mr Lee's intention to comply with the site attendance policy through other means of identity verification.

In the final consideration, the Full Bench noted that there was no evidence indicating management at Superior Wood Pty Ltd ever considered alternate strategies for payroll efficiencies. Notwithstanding this, the manual sign-in system remained in use long after the dismissal of Mr Lee. The Full Bench, therefore, concluded that the timing of the dismissal of Mr Lee was difficult to explain (again in line with a coercive style of management). In addition, whilst the claim of accuracy and fraud was raised regarding not using the biometric fingerprint scanner, no evidence was provided by management to support this line of argument or that Mr Lee was a risk in relation to inaccurate timekeeping or fraud. Instead, the Full Bench noted that the evidence tended to side with the contrary view. The Full Bench stated that the risk of not knowing where Mr Lee was in the event of an emergency was overstated. The site was very large and the nature of signing in via a fingerprint scanner would not have accounted for an employee's location at any point in time. Indeed, an emergency during the period where both manual and fingerprint scanner processes were in operation (a fire alarm sounding) indicated that a combination of fingerprint scanner and manual records were adequate in identifying who was on site. As such, the argument to the Full Bench that Mr Lee's fingerprint was necessary as a means of attendance record-keeping and of accounting for safety of employees was not compelling.

A concluding point which emerged for future consideration was indeed that of boundary management, through the requirement of the need for a higher level of consent regarding the collection of biometric data. Mr Lee sought to have the Full Bench adjudicate on this point. The Full Bench pointed out that this was outside the specific issues of this case. However, the Full Bench concluded that there was no evidence that any of the entities had mechanisms in place to protect and manage biometric information collected in ways consistent with the Privacy Act. As noted by Altman (1975), Westin (1967) and Petronio (2002), the nature of (informational) privacy is dynamic and operates through individual, group, organisational and institutional levels. Tensions arise when the balance in the systems and structures of privacy boundaries is disturbed or poorly managed (Margulis, 2003; Westin, 1967): in this case, through a lack of understanding of the boundaries by both the employer and employees of the significance of providing biodata and its poor security. The overturning of the decision indicates that the boundaries

of informational privacy of employees can and should be expected to be managed effectively and responsibly. As noted by Altman (1975) regarding the bi-directionality of the relationship, and highlighted here by Mr Lee, it is also the responsibility of the employees to understand the significance of checks and balances in providing their unique biodata. This case helps to increase the legal boundaries and guidance in building robust and fair policies and in theory reduce the turbulence at the boundaries of these issues within the system, not least as these technologies become more available, and to build trust in the management of these issues in the workplace. This case and the notion of the collection and protection of biometric data are an ever-increasing critical issue for a growing number of the working population.

Conclusions

In dealing with issues of managerial prerogative, employee privacy rights and biometric data, this case highlights an emerging contested terrain and boundaries in the employment relationship associated with the collection, use, storage and management of biometric data at the workplace. Reflecting on the fluidity of these boundaries around such a sensitive workplace issue highlights what Petronio (1991) describes as ‘boundary opening’ and ‘boundary closure’, in that had Mr Lee initially agreed to the taking of biometric information (boundary opening), and then reneged, his rights would have been covered by a different law and he would not have had the opportunity for redress or closure of this information flow. Noting the EU definition of biometric data as a special category of personal data, we would argue that such significant and unique personal data need to be more clearly protected and managed.

Whilst this case has helped to highlight, identify and clarify the clear need to protect individual biometric data and privacy from arbitrary or unlawful interference in the workplace, the appeal and subsequent overturning of the dismissal provides an improved framework to guide organisations in providing a fair and balanced approach to the collection and use of employees’ biometric data. This, we argue, cannot be underestimated. The fundamental questions in this context in challenging these boundaries are, firstly, *why* organisations have decided to implement biometrics and the understanding or lack thereof of the implication for collection of such personal data. Secondly, why the law has yet to address this emerging and significant issue in the data capture and surveillance of employees in standalone legislation, particularly in protecting both the employee’s rights and the employer from legal action, is surprising. As the Full Bench stated, Mr Lee was entitled to seek protection of his biometric characteristics. However, as noted, had he initially agreed to the taking of his fingerprint (even though he was not provided with the appropriate information), he would not have had the protection of the privacy legislation. This haphazard approach to boundary management needs to be addressed with a clear legal framework which would provide better understanding of the issues and implications for all stakeholders to ensure all available information is consulted, and the practicalities of biometrics are fully understood, before the employee chooses to give such personal data.

Declaration of conflicting interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

ORCID iDs

Peter Holland  <https://orcid.org/0000-0001-7256-2545>

Tse Leng Tham  <https://orcid.org/0000-0003-1729-823X>

References

- Alder S and Ambrose M (2005) Toward understanding fairness judgements associated with computer performance monitoring: An integration of the feedback, justice, and monitoring research. *Human Resource Management Review* 15(1): 43–67.
- Allen M, Coopman Hart J and Walker K (2007) Workplace surveillance and managing privacy boundaries. *Management Communication Quarterly* 21(2): 172–200.
- Altman I (1975) *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Monterey, CA: Brooks/Cole.
- Altman I (1990) Towards a transactional perspective: A personal journey. In: Altman I and Christensen K (eds) *Environment and Behavior Studies: Emergence of Intellectual Traditions*. New York: Plenum, pp. 335–355.
- Aponovich D (2001) Case study: Biometrics eases city's network access, security woes. *Datamation*. Available at: www.datamation.com/secu/article.php/863861/Case-StudyBiometrics-Eases-Citys-Network-Access-Security-Woes.htm
- Ball K (2010) Workplace surveillance: An overview. *Labor History* 51(1): 87–106.
- Ball K, Daniel EM and Stride C (2012) Dimensions of employee privacy: An empirical study. *Information Technology & People* 25(4): 376–394.
- Barbeler D (2018) Turn on, tune in, drop out. *HRMonthly*, June, pp. 12–17.
- Barnes A, Balnave N and Holland P (2018) 'Utterly disgraceful': Social media and the workplace. *Australian Journal of Public Administration* 77 (3): 492–499.
- Bolle R, Connell J, Pankanti S et al. (2004) *Guide to Biometrics*. New York: Springer.
- Carpenter D, McLeod A, Hicks C and Maasberg M (2016) Privacy and biometrics: An empirical examination of employee concerns. *Information Systems Frontiers* 20(1): 91–110.
- Chang SE, Lui A and Lin S (2015) Exploring employee privacy and trust for employee monitoring. *Industrial Management and Data Systems* 115(1): 86–106.
- Currah P and Mulqueen T (2011) Securitizing gender: Identity, biometrics and transgender bodies at the airport. *Social Research* 78(2): 557–582.
- Dantcheva A, Elia P and Ross A (2015) What else does your biometric data reveal? A survey on soft biometrics. *IEEE Transactions on Information Forensics and Security* 1(3): 441–467.
- Determann L and Sprague R (2011) Intrusive monitoring: Employee privacy expectations are reasonable in Europe, destroyed in the United States. *Berkeley Technology Law* 26(2): 979–1036.

- Du E, Yang K and Zhou Z (2011) Key incorporation scheme for cancellable biometrics. *Journal of Information Security* 2(4): 185–194.
- Fairweather N (1999) Surveillance in employment – the case of teleworking. *Journal of Business Ethics* 22(2): 39–49.
- Gemalto (2019) *Biometric Data and Data Protection Regulations*. Paris: Gemalto, NV.
- Holland P, Cooper B and Hecker R (2015) Electronic monitoring and surveillance in the workplace: The effects on trust in management, and the moderating role of occupational type. *Personnel Review* 44(1): 1–27.
- Holland P, Cooper B and Hecker R (2016) Social media: The new employee voice? *International Journal of Human Resource Management* 27(21): 2621–2634.
- Hugl U (2013) Workplace surveillance: Examining current instruments, limitations and legal background issues. *Tourism & Management Studies* 9(1): 58–63.
- Hussain A (2015) Using biometric identification technology to combat time theft in workforce management. Available at: www.m2sys.com/blog/workforce-management/using-biometricidentification-technology-combat-time-theft-workforce-management/
- Jackson L (2009) Biometric technology: The future of identity assurance and authentication in the lodging industry. *International Journal of Contemporary Hospitality Management* 21(7): 892–905.
- Kelly D and Herbert W (2004) When James Bond enters the workplace: Use and abuses of technology – A guide for in-house counsel and litigators. Available at: www.bna.com/bnabooks/ababna/annual/2004/kelly.doc
- Krishnan R and Mostafavi R (2018) Biometric technology: Security and privacy concerns, *Journal of Internet Law* 22(1): 19–23.
- Lane FS (2003) *The Naked Employee: How Technology is Compromising Workplace Privacy*. New York: Amacom.
- Lee J v. Superior Wood Pty Ltd T/A Superior Wood, (FWC 4762), November 2018.
- Lee J v. Superior Wood Pty Ltd t./a Superior Wood, (FWC 95), January 2019.
- Lee J v. Superior Wood Pty Ltd, (FWCFB 2946), May 2019.
- Magnet S (2011) *When Biometrics Fail: Gender, Race, and the Technology of Identity*. Durham, NC: Duke University Press.
- Margulis S (2003) On the status and contribution of Westin's and Altman's theories of privacy. *Social Issues* 59(2): 411–429.
- Martin A, Wellen J and Grimmer M (2016) An eye on your work: How empowerment affects the relationship between electronic surveillance and counterproductive work behaviours. *International Journal of Human Resource Management* 27(21): 2635–2651.
- Mason D, Button G, Lankshear G et al. (2002) On the poverty of apriorism: Technology, surveillance in the workplace and employee responses. *Information, Communication and Society* 5(4): 555–572.
- Moradoff N (2010) Biometrics: Proliferation and constraints to emerging and new technologies. *Security Journal* 23(4): 276–298.
- Nanavati S, Thieme M and Nanavati R (2002) *Biometrics: Identity Verification in a Networked World*. New York: John Wiley.
- Norris-Jones L (2012) Biometric access control in the workplace: Benefit or bind? *International Journal of Information Technology and Management* 11(1/2): 61–71.
- Petronio S (1991) Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Communication Theory* 1(11): 311–335.

- Petronio S (2002) *Boundary of Privacy: Dialectics of Disclosure*. New York: SUNY Press.
- Petronio S, Ellemers N, Giles H and Gallois C (1998) (Mis)communicating across boundaries. *Communication Research* 61: 101–113.
- Qantas Airways Limited v. Transport Workers' Union of Australia* (2003) PR928229, 27 February.
- Rao U (2018) Biometric bodies, or how to make electronic fingerprinting work in India. *Body and Society* 24(3): 68–94.
- Roberg-Perez S (2017) The future is now: Biometric information and data privacy. *Antitrust* 31(3): 60–65.
- Schneider B (2015) *The Hidden Battles to Collect Your Data and Control Your World*. New York: W.W. Norton.
- Schumann A and Monari E (2014), A soft-biometrics dataset for person tracking and re-identification. In: *11th IEEE International Conference on Advanced Video and Signal Based Surveillance* (AVSS), Seoul, Korea, 26–29 August 2014.
- Sewell G and Barker JR (2006) Coercion versus care: Using irony to make sense of organizational surveillance. *Academy of Management Review* 31(4): 934–961.
- Stewart L (2019) Big data discrimination: Maintaining protection of individual privacy without disincentivizing businesses' use of biometric data to enhance security. *Boston College Law Review* 60(1): 349–386.
- Stratton J and Stam K (2003) Information technology, privacy and power within organizations: A view from boundary theory and social exchange perspectives. *Surveillance and Society* 1(2): 152–190.
- The Privacy Act 1988, Cth. Canberra. Australia: OAIC.
- Westin AF (1967) *Privacy and Freedom*. New York: Athenaeum Press.
- Woolworths Ltd (t/as Safeway) v. Brown* 145 AIRC, September 2005.
- WPX (Workplace Express) (2003) Finger scan plans fail to get off ground. Sydney, Australia.
- York A and Carty L (2006) *Privacy: Biometric Technology and Privacy in the Workplace*. Available at: www.blakes.com/english/publications/businesswithcanada/bwc/html/article.asp?article=413
- Zhai X and Qui R (2010) The status quo and ethical governance in biometrics in mainland China. In: Kumar A and Zhang D (eds) *Ethics and Policy of Biometrics*. Berlin and Heidelberg: Springer, pp. 127–137.
- Zielinski D (2018) Use of biometric data grows, though not without legal risks. *HRNews*. Available at: <https://search.proquest.com/docview/2092540945?accountid=13552>

Author biographies

Peter Holland is a Professor of Human Resource Management and Director of the Executive MBA at Swinburne University of Technology, Melbourne. Peter has worked in the Australian finance sector and consulted to the private and public sector in areas related to human resource management and employee relations. His current research interests include employee voice and silence, workplace electronic monitoring and surveillance and talent management. He has authored/coauthored 12 books and over 150 journal articles, monographs and book chapters on a variety of human resource management and employee relations issues.

Tse Leng Tham is a Lecturer of Human Resource Management at the School of Management, RMIT University, with a PhD from Monash University, Australia. Her research interests include workplace surveillance, well-being, workplace climate and voice. She has published in *Human*

