DECISION

Fair Work Act 2009
s 604—Appeal of decision

Jeremy Lee
v
Superior Wood Pty Ltd t/a Superior Wood
(C2018/6600)

DEPUTY PRESIDENT SAMS
DEPUTY PRESIDENT GOSTENCNIK
COMMISSIONER MCKINNON

SYDNEY, 17 JANUARY 2019

Application for permission to appeal and appeal against a decision of Commissioner Hunt issued at Brisbane on 1 November 2018 in matter U2018/2253 – unfair dismissal application dismissed – valid reason found – refusal of employee to use biometric fingerprint scanning to record site attendance – failure to comply with lawful and reasonable policy direction – dismissal not harsh, unjust or unreasonable – arguable case of appealable error – grounds of appeal raise important, novel and emerging issues in the Commission's unfair dismissal jurisdiction – permission to appeal granted – further proceedings to be programmed.

INTRODUCTION

[1] Mr Jeremy Stuart Lee ('the appellant') has lodged an application for permission to appeal and appeal against a decision of Commissioner Hunt issued at Brisbane on 1 November 2018, in which the Commissioner found the appellant's dismissal by Superior Wood Pty Ltd t/a Superior Wood ('Superior Wood' or 'the respondent') on 12 February 2018, was not '*harsh, unjust or unreasonable*', and therefore not unfair, within the meaning of s 387 of the *Fair Work Act 2009* ('the Act'). Accordingly, she dismissed his application for an unfair dismissal remedy; see: *Jeremy Lee v Superior Wood Pty Ltd* [2018] FWC 4762 ('the Decision'). The appellant contends in his appeal that the Commissioner erred in a number of respects, which we will detail later in this decision.

[2] Shortly stated, the Commissioner found that the appellant's dismissal was not unfair in that he refused to follow a lawful and reasonable workplace policy; specifically, his refusal to use the respondent's biometric fingerprint scanners in accordance with the Site Attendance Policy (the 'Policy'), which were introduced as a safety measure to record an employee being

on site. The appellant maintains that as he owns the biometric data collected and stored by the scanners, and as it is sensitive personal information, it cannot be obtained by the employer, without his consent. His refusal to give consent triggered his dismissal for the reasons set out in the Commissioner's Decision. He also maintains that the respondent's relevant Policy is in breach of the *Privacy Act 1988 ('Privacy Act')* and the Commissioner erred in not finding this to be case.

[3] The appeal was listed before the Full Bench of the Commission on 11 December 2018 in Sydney. The appellant appeared for himself by video link from Brisbane (noting he was represented by Counsel in the original proceeding). Mr A Herbert of Counsel appeared for the respondent, with permission for Superior Wood to be legally represented having been earlier granted by the Full Bench, pursuant to s 596 of the Act. We note Mr Herbert had also appeared in the original proceedings.

[4] At the outset of the proceedings, it was apparent that the appellant had not filed any submissions in support of his appeal. He claimed he had been unaware of the requirement to do so, or to attend the hearing to argue his case. Despite the appellant conceding he had simply not read the Notice of Listing or the Directions sent to him on 27 November 2018, the Full Bench offered him an opportunity to file written submissions and the matter would be determined 'on the papers', or in the alternative, he could have a short adjournment to consider the discrete question of permission to appeal and the matter would proceed later in the day. He chose the latter option, and we resumed the hearing shortly thereafter.

EMPLOYMENT BACKGROUND AND COMPANY OPERATIONS

[5] Superior Wood operates two sawmills at Melawondi and Imbil, Queensland. About 400 employees worked at the Imbil site. The appellant was employed at the time of his dismissal at Imbil Mill, and had been employed as a casual General Hand for a period of approximately 3 ¼ years at both sites.

[6] In October 2017, the respondent announced that it was introducing the biometric scanners at the Imbil site to record on-site presence. From the outset, the appellant objected to the use of the scanners and refused to use them. He was the only employee who did so. Between November 2017 and February 2018, a number of meetings were held between the

appellant and the respondent's managers to discuss his concerns, but he steadfastly maintained his refusal to use the scanners and proposed that he continue to use the 'paper sign-in' process or a swipe card system. The respondent insisted that all employees use the scanners as it would be impractical to allow one employee to be exempt from an improved safety measure, when all other employees had agreed to do so. There was some dispute in the appeal about the nature of the consent given by the remainder of the workforce, but we need not take this matter any further at this point.

THE DECISION

[7] The Commissioner's consideration and conclusions as to whether the appellant's dismissal was '*harsh, unjust or unreasonable*' are set out from [193] to [247] of the Decision. In respect to valid reason, the Commissioner framed her finding based on two questions:

(a) whether the collection of the appellant's biometric information was inconsistent with the respondent's obligations under the Privacy Act; and
(b) whether the introduction of the Site Attendance Policy was unjust or unreasonable.

[8] It is apparent that the appellant's focus in this appeal was his claim that the Commissioner's finding of a valid reason was an error.

[9] As to the second question, and after considering the decision in *Woolworths v Brown* (2005) 145 IR 284 at 297, the Commissioner found at [198] – [199] as follows:

> "[198] In light of the Full Bench's decision in Woolworths, I consider that the Site Attendance Policy is not unjust or unreasonable. It is entirely reasonable for the employer to improve upon an inherently unsafe obligation to run to the front administration office in the event of an emergency, locate a paper sign-on sheet and attempt to ascertain who is at work over a site of significant size. On the evidence before the Commission, supervisors can immediately see who from their area of work is present in the workplace using the information collected through adherence to the Site Attendance Policy and displayed on a supervisor's phone.
>
> [199] Further, the improved integrity and efficiency of the payroll across the Finlayson Group is a persuasive matter to find that the introduction of the Site Attendance Policy was neither unjust or unreasonable. I find that Superior Wood either directly or through its related body corporate entities held a right to manage its

affairs by the introduction of the Site Attendance Policy, requiring all individuals who work at the various premises to comply with it. I would not accept that an individual's refusal to comply with the policy would render any subsequent dismissal, with adequate caution, invalid."

[10] In respect to the *Privacy Act* question, the Commissioner summarised the relevant provisions of the *Privacy Act* at [128] and [129] as follows:

"[128] Section 15 of the Privacy Act provides that an APP entity must not do an act, or engage in a practice that breaches an APP. Section 6A of the Privacy Act provides that an act or practice breaches an APP if, and only if, it is contrary to, or inconsistent with that principle.

[129] The APP's are set out in Schedule 1 to the Privacy Act. There are 13 of them. APP1 requires APP entities to take reasonable steps to implement practices, procedures, and systems relating to their functions or activities that will ensure compliance with the APPs and enable them to deal with inquiries or complaints about compliance with the APPs. APP1 compels APP entities to have clear and up-to-date privacy policies about the management of personal information by the entity. APP1 is produced below:

"1 Australian Privacy Principle 1--open and transparent management of personal information

1.1 The object of this principle is to ensure that APP entities manage personal information in an open and transparent way.

Compliance with the Australian Privacy Principles etc.

1.2 An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:

(a) will ensure that the entity complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity; and
(b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles or such a code.

APP Privacy policy

1.3 An APP entity must have a clearly expressed and up-to-date policy (the APP privacy policy) about the management of personal information by the entity.

1.4 Without limiting subclause 1.3, the APP privacy policy of the APP entity must contain the following information:

(a) the kinds of personal information that the entity collects and holds;

(b) how the entity collects and holds personal information;

(c) the purposes for which the entity collects, holds, uses and discloses personal information;

(d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;

(e) how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(f) whether the entity is likely to disclose personal information to overseas recipients;

(g) if the entity is likely to disclose personal information to overseas recipients--the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

Availability of APP privacy policy etc.

1.5 An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available:

(a) free of charge; and

(b) in such form as is appropriate.

Note: An APP entity will usually make its APP privacy policy available on the entity's website.

1.6 If a person or body requests a copy of the APP privacy policy of an APP entity in a particular form, the entity must take such steps as are reasonable in the circumstances to give the person or body a copy in that form.

*APP is an acronym for 'Australian Privacy Principles'.

[11] The Commissioner considered that the respondent was bound by the *Privacy Act* and found at [201] – [204]:

"[201] Superior Wood meets the definition of an 'organisation' and an 'APP entity' under the Privacy Act. It is not contested by the parties that Superior Wood is an APP entity and is obliged to adhere to the APPs. Pursuant to APP 3.3, Superior Wood must not collect sensitive information about an individual unless the individual consents to

the collection of the information and the information is reasonably necessary for one or more of the entity's functions or activities.

[202] The meaning of the word 'consent' as it appears within APP 3.3 is defined by section 6 of the Privacy Act which states that 'consent', "means express or implied consent".

[203] Having regard to the issue of whether the introduction of biometric scanners at the Superior Wood premises is 'reasonably necessary', I have no hesitation in so finding. For the same reasons stated earlier, the Finlayson Group wished to consolidate its payroll. Superior Wood was the last entity to have the scanners introduced, and after a suitable period of time where there was duplication, it was a reasonable course for the employer to then remove the paper payroll system to join in with its parent entity activities. Once Superior Wood and the Finlayson Group was satisfied the biometric scanning was properly implemented, the entities wished to do away with all manual payroll handling. Once that decision was made, I do then consider the collection of the biometric information to be reasonably necessary for its functions or activities.

[204] On a fairness and reasonableness consideration, I am minded to side with the views of management of Superior Wood that having Mr Lee use some alternative method such as a swipe pass or continue to use a paper sign-on would be inefficient, inequitable, and a burden. Requiring a manual pay run to be implemented for a single employee, as against either 150 employees or 400 employees in the group would be an onerous obligation."

[12] The Commissioner then concluded that all the other employees had given 'implied consent' to the collection of their sensitive information, by registering their fingerprint algorithms during November 2017. However, the Commissioner was critical of the respondent for firstly, not providing employees with a 'collection notice' stating how it would keep the information safe; and secondly, having no privacy policy in place in 2017, despite the *Privacy Act* being applicable to it since 2001. There was some discussion about which entity gathered the scanned information. The Commissioner found at [220]–[223]:

"[220] I consider that the exemption under s.7B(3) of the *Privacy Act* would apply to the non-exhaustive list of employee records, if the record had been obtained or held. Many employers have been using biometric data for decades or more, and it would be highly improbable that each of those employers owned the scanning equipment, the servers on which the data was held, or had any relationship with the provider of the biometric system the employer had installed.

[221] The reference in the employee exemption is to the record having been held, and following it being held, it is exempt.

[222] In my view, the employee record exemption does not ameliorate the obligation by Superior Wood to issue to Mr Lee and other employees a privacy collection notice.

> [223] It follows that Superior Wood was not exempt from complying with APP 3.3 in collecting its employees sensitive information, and that it could not have collected Mr Lee's sensitive information in the circumstances where he did not consent to Superior Wood collecting his sensitive information."

[13] We reference the exemption for employee records under s 7B(3) of the *Privacy Act*:

> "(3) An act done, or practice engaged in, by an organisation that is or was an employer of an individual, is ***exempt*** for the purposes of paragraph 7(1)(ee) if the act or practice is directly related to:
>
> (a) a current or former employment relationship between the employer and the individual; and
>
> (b) an employee record held by the organisation and relating to the individual."

[14] At [225]–[228], the Commissioner discussed the appellant's alternative proposals for demonstrating his attendance on site and found:

> "[225] Superior Wood could not lawfully force Mr Lee to consent to the collection of his sensitive information and to comply with the Site Attendance Policy. It did not do so. It informed him that if his consent was not forthcoming, and he failed to comply with the Site Attendance Policy, dismissal was a likely outcome. It failed to inform Mr Lee pursuant to the Privacy Act of the responsibilities it and other associated entities would meet.
>
> [226] It is apparent from the evidence that Mr Lee made a concerted effort to identify alternatives methods of identification and site attendance verification that Superior Wood could implement for his use, rather than complying with the Site Attendance Policy and using the scanner. Mr Lee did not object to the purpose of the Site Attendance Policy, but the collection of his biometric information and particularly that information which related to Mr Lee's fingerprint.
>
> [227] There is no evidence that Superior Wood took any steps to evaluate the costs of any if the alternative methods of identification put forward by Mr Lee. Superior Wood has always maintained that the use of the scanners and compliance with the Site Attendance Policy is mandatory for employment with Superior Wood.
>
> [228] I accept that methods of employee identification and attendance verification other than biometric scanners are available, some of which were put forward as alternatives to the scanners by Mr Lee on 18 January 2018. However, I consider that many of those other methods do not provide the same degree of certainty of identity verification as the scanners used in Superior Wood's workplace."

[15] At [233]–[235], the Commissioner concluded as follows:

> "[233] I do not accept that the employer's failure to provide a privacy collection notice to its employees prior to obtaining their personal and sensitive information, in all the circumstances before me, constitutes the Site Attendance Policy being rendered unlawful. While there may have been a breach of the Privacy Act relevant to the notice given to employees, the private and sensitive information was not collected and would never be collected relevant to Mr Lee because of his steadfast refusal. The policy itself is not unlawful, simply the manner in which the employer went about trying to obtain consent may have constituted a breach of the Privacy Act. Any such breach might constitute a matter that could be examined by the Australian Information Commissioner and Privacy Commissioner.
>
> [234] It mattered not who owned the equipment, Mr Lee would never provide his consent. Mr Lee refused to provide his consent, which he is entitled to do. He did, however, then fail [*sic*] to meet his employer's reasonable request to implement a fair and reasonable workplace policy.
>
> [235] In all the circumstances, and having regard to any potential breaches of the Privacy Act, I find there was a valid reason for the dismissal."

[16] As we do not understand there to be any relevant challenge to the Commissioner's other findings under ss (b) – (g) of s 387 of the Act, we need not restate them. However, under ss (h) 'other matters', the Commissioner said at [243] – [245]:

> "[243] Mr Lee's decision to agree to the use of his biometric data, or even his DNA in other scenarios puts his refusal to use the biometric scanner at Superior Wood somewhat at odds.
>
> [244] His evidence is that he would provide a urine sample to a pathology laboratory contracted by his employer, without much concern. It is my view that if an employee held concerns a contracted organisation could, for example, place them somewhere they were not, it would be far easier to do so with an actual urine sample, as opposed to a reconstructed fingerprint.
>
> [245] Mr Lee might be a conscientious objector to his biometric data being used by an employer, the employer's parent company, and a third party supplier. His objection was unreasonable when taking into consideration the purposes of the Site Attendance Policy, the improvements to payroll and health and safety, and the alternatives that would have been required to have been put in place for him."

[17] The Commissioner then set out a long, detailed speech given by the Deputy Privacy Commissioner on 27 May 2010 about biometric data collection. It is unnecessary, for present purposes, for us to reproduce this speech – informative as it was.

GROUNDS OF APPEAL

[18] We set out the appellant's grounds of appeal as set out in his Notice of Appeal (as written):

> "The case is about Superior Wood's refusal to recognise that I own my biometric data.
>
> The Commissioners ruling also refuses to recognize that I own my biometric data.
>
> In other words the case is about ownership.
>
> By allowing Superior to sack me for refusing consent, the decision overrules my ownership.
>
> The decision was in error because it allows the dismissal of an employee for protecting ownership of their sensitive information. That is a harsh, unjust and unreasonable dismissal.
> Mistake in the Facts.
>
> The ruling relies heavily on the claim that the new scanner system improves safety. This claim is used to assert that Superior acted reasonably by making it site attendance policy, and therefore mandatory.
>
> [245] …"taking into consideration the purposes of the site attendance policy, the improvements to payroll and health and safety…"
>
> [235] …"having regard to any potential breaches of the Privacy Act, I find there was a valid reason for the dismissal."
>
> [229] " I note that the scanners allowed for additional safety benefits beyond simple attendance verification, such as reviewing site attendance on supervisors phones."
>
> The Commissioner believes use of the scanner improves safety. This is incorrect. A paper sign in book was used by the employer during a fire alarm site evacuation to check off those employees on site. This old system was used in preference to the already operational scanner system. This proves that in reality, even the employer did not consider that the new scanner system improved site safety.
>
> Further, the scanner system cannot be used to determine workers location. All it does is display scan in and scan off times, which are the same as sign in and sign off times under the old paper system.
>
> From [216] "Mr Lee's biometric data was not collected as he did not provide his consent…Mr Lee said he did not consent…"
>
> This is incorrect. I was never asked for my consent. Superior actively ducked the issue as it acknowledges ownership.
>
> From [225] "Superior…informed him that if his consent was not forthcoming, and he failed to comply with the site attendance policy, dismissal was a likely outcome."

This is wrong. Superior never asked for or mentioned consent. I refused to provide my biometric data.

By describing it this way, the commission has also sidestepped the issue of ownership.

Errors in Judgement.

The Commissioner found the introduction of biometric scanners, (which require the collection of workers "sensitive information"), to be "reasonably necessary", even though their use involved collection of biometric data, workers were not informed or asked beforehand, and the business is perfectly capable of operation without biometric scanners.

[216] "an entity must collect personal information only by lawful and fair means."

The commissioner ignores that employees biometric data WAS collected by unlawful (Superior breached the Privacy Act) and unfair (Superior made collection of biometric data site policy) means.

Collection of my data was attempted under threat of being sacked. Furthermore, Superior provided no collection notices, no assurances as to handling of that data, and other entities were given access. In so doing, Superior breached the Privacy Act.

Superior threatened me with termination to collect my biometric data, yet the commissioner ruled that "lawful and fair".

[202] 'Consent' is defined by the Privacy Act "means express or implied consent"

[205] "… it appears that the other employees of superior gave implied consent… by registering their fingerprint"

[209] "It is argued that because Mr Lee's biometric data is never collected, there was never a breach with respect to Mr Lee."

[210] "…his sensitive information"

[216] "Mr Lee's biometric data was not collected, as he did not provide his consent. Mr Lee said he did not consent and therefore Superior did not collect personal information."

[234] "Mr Lee refused to provide his consent, which he is entitled to do."

In summary:

The ruling states consent is implied by providing a scan.

The ruling also says my privacy can only be breached if I provide a scan.

Yet providing a scan implies consent.

Taken together, this means that a breach of my privacy is impossible.

This same logic is applied throughout and undermines the possibility of a fair ruling.

Similarly, the commissioner's suggestion [210] is that this sensitive information is mine, but the decision approves of my sacking when I refused consent.

The commission cannot hold both positions to be true. Either I own my biometric data and have the right to refuse or I don't own it and Superior can fairly sack me for not providing it."

[19] In respect to permission to appeal, the appellant said at 3.1 of the Notice to Appeal:

"There is clear public interest in this decision because:

a. It is a test of Australian workers rights to privacy and ownership of their sensitive information.

b. It has obvious ramifications as the Commissioner has ruled that an employee cannot refuse to give their sensitive information to an employer and be protected from dismissal.

c. This decision means that all employers may legally sack employees for refusing to provide their sensitive information.

d. This decision grants employers the right to claim ownership of employees sensitive information and the right to discriminate against employees who wish to maintain ownership of their sensitive information.

e. This decision changes the nature of the relationship between employer/employee from an exchange of labour to one which includes the collection of employees sensitive information.

f. The ruling sets a precedent . This ruling legitimizes and legalizes the taking of employees sensitive information by employers."

SUBMISSIONS

[20] In **oral submissions**, the appellant developed his argument about a person's 'ownership' of their biometric data and that as this is a matter affecting every Australian worker, the question of an employer's right to dismiss an employee for refusing to provide their personal data, must attract the public interest. He drew a comparison to the present public controversy concerning the Australian Government's collection of a person's 'My Health records'. He put that there can be no guarantee that personal data collected by

Governments or employers would not fall into the wrong hands and be used improperly, for example, to create false identities.

For Superior Wood

[21] Mr Herbert referred to the principles dealing with permission to appeal and adopted the conventional approach, as set out in the recent Full Bench decision in *Morgan v Serco Australia Pty Limited* [2018] FWC 7011.

[22] Mr Herbert addressed a number of the appellant's contentions as to errors in the Decision. Contrary to his claim that the Commissioner incorrectly found the use of the scanner improved safety, the Commissioner had expressly set out some of these improvements; notably that if there is a fire on site, supervisors have access to the scanner system in real time, as to who is on site. This also applies if an emergency service person risks entering the site in a fire to find persons, who may not be there. Further, it is difficult to understand how the Commissioner was said to have erred in finding that the appellant's biometric data was not collected when he did not provide consent.

[23] Further, Mr Herbert said that a supervisor had not informed the appellant that if his consent was not forthcoming and he failed to comply with the Policy, dismissal was the likely outcome, because he had always refused consent and continues to do so. To suggest this was an error, much less a significant error, was just 'playing with words'.

[24] In questioning from the Bench, Mr Herbert outlined the provisions of the *Privacy Act* and which provide for an exemption at s 7B(3) for employee records. Mr Herbert contended that there is no distinction between an employee record already in existence and the process to create a record; in this case by seeking an employee's consent. He conceded that the Commissioner did not make a direct finding that an act or practice, directly related to an employment relationship and an employee record held, also extends to the means of obtaining that record; see [220] of the Decision.

[25] Mr Herbert said the question as to the lawfulness of the respondent's obtaining of the biometric data was irrelevant, because the appellant was never going to provide his consent, whether it was lawful or not. Put another way, if the only issue was the respondent's failure to

provide written notice to the employees, and a process was undertaken to correct that error, the appellant's steadfast refusal to comply with the Policy would not have changed the outcome. This would ultimately be a fruitless exercise, thereby serving no public utility if permission to appeal was granted on that basis and the appellant was ultimately reinstated, but still refused to consent to his biometric collection, which he insisted he would.

[26] Mr Herbert submitted that the concerns of the appellant as to what happens once the data is collected and stored, are answered by the employee records exemption in the *Privacy Act*. Further, this case is of no interest or significance to anyone other than the appellant's own interests, least of all to any of the other employees of Superior Wood, who have all complied with the Policy.

[27] In **reply**, the appellant submitted that the scanning system provided no greater protection for employees than a 'paper sign-in' system. In any event, any system can be 'hacked into' and no system provides a perfect guarantee. He insisted the scanning system does not improve safety.

[28] The appellant queried the validity of the consent given by the rest of the workforce, in circumstances where they were aware they would have been terminated if they did not provide their biometric data. This could not be regarded as consent, but coercion. Furthermore, employees were never asked for their consent or made aware of their rights under the *Privacy Act*.

CONSIDERATION

Approach on permission to appeal

[29] As we previously noted, these proceedings deal only with permission to appeal considerations. While the appellant provided no written submissions and for the most part argued the merits of his appeal, we consider his oral submissions provided him the opportunity to sufficiently address the questions we must determine at this point, of whether it is in the public interest to grant permission to appeal of the Decision and, in doing so, whether an arguable case of relevant error has been made out.

[30] An appeal under s 604 of the Act is an appeal by way of rehearing and the Commission's powers on appeal are only exercisable if there is error on the part of the primary decision maker (this is so because on appeal the Commission has power to receive further evidence, pursuant to s.607(2); see *Coal and Allied v AIRC* (2000) 203 CLR 194 at [17] per Gleeson CJ, Gaudron and Hayne JJ). There is no right to appeal and an appeal may only be made with the permission of the Commission.

[31] This appeal is one to which s 400 of the Act applies. Under s 400, the Commission must not grant permission to appeal from a decision made by the Commission in relation to unfair dismissal unless it considers it in the public interest to do so. An appeal of an unfair dismissal decision involving a question of fact can only be made on the ground that the decision involved a significant error of fact.

[32] In *Coal & Allied Mining Services Pty Ltd v Lawler and others* (2011) 192 FCR 78 at [43], Buchanan J (with whom Marshall and Cowdroy JJ agreed) characterised the test under s 400 as "a stringent one". The task of assessing whether the public interest test is met is a discretionary one involving a broad value judgment; see: *O'Sullivan v Farrer* (1989) 168 CLR 210 per *Mason* CJ, *Brennan*, *Dawson* and *Gaudron* JJ; applied in *Hogan v Hinch* (2011) 85 ALJR 398 at [69] per *Gummow*, *Hayne*, *Heydon*, *Crennan*, *Kiefel* and *Bell* JJ; *Coal & Allied Mining Services Pty Ltd v Lawler and others* (2011) 192 FCR 78 at [44] -[46]. In *GlaxoSmithKline Australia Pty Ltd v Makin* [2010] FWAFB 5343, 197 IR 266 at [27], a Full Bench of the Commission identified some of the considerations that may attract the public interest:

> "... the public interest might be attracted where a matter raises issues of importance and general application, or where there is a diversity of decisions at first instance so that guidance from an appellate court is required, or where the decision at first instance manifests an injustice, or the result is counter intuitive, or that the legal principles applied appear disharmonious when compared with other recent decisions dealing with similar matters."

[33] It will rarely be appropriate to grant permission to appeal unless an arguable case of appealable error is demonstrated. This is so because an appeal cannot succeed in the absence of appealable error; see: *Wan v AIRC* (2001) 116 FCR 481 at [30]. However, the fact that the Member at first instance made an error is not necessarily a sufficient basis for the grant of permission to appeal; see: *GlaxoSmithKline Australia Pty Ltd v Makin* [2010] FWAFB 5343

at [26]-[27], 197 IR 266; *Lawrence v Coal & Allied Mining Services Pty Ltd t/as Mt Thorley Operations/Warkworth* [2010] FWAFB 10089 at [28], 202 IR 388, affirmed on judicial review in *Coal & Allied Mining Services Pty Ltd v Lawler* (2011) 192 FCR 78; *NSW Bar Association v Brett McAuliffe; Commonwealth of Australia represented by the Australian Taxation Office* [2014] FWCFB 1663 at [28].

[34] An application for permission to appeal is not a de facto or preliminary hearing of the appeal. In determining whether permission to appeal should be granted, it is unnecessary and inappropriate for the Full Bench to conduct a detailed examination of the grounds of appeal; see: *Trustee for The MTGI Trust v Johnston* [2016] FCAFC 140 at [82].

[35] It is unnecessary for us to consider, in detail, the grounds of appeal set out in the appellant's Notice of Appeal and his argued oral submissions. Given the considerations which go to the public interest, we have decided to grant permission to appeal for the following reasons:

> (1) We are persuaded that there is an arguable case of appealable error identified in the appeal as to:
>
> > (a) whether the request to comply with the respondent's Site Attendance Policy was lawful and/or reasonable, in all the circumstances of the case, and in the context of the appellant's refusal to provide consent to the disclosure of his personal biometric data;
> >
> > (b) whether the Commissioner's findings as to the application of the *Privacy Act* were relevant, and/or appropriately balanced with the exercise of the Commissioner's discretion under Part 3-2 of the Act – Unfair Dismissal;
> >
> > (c) to the extent the *Privacy Act* is relevant, whether the exemption in s 7B in respect to an '*employee record held by the organisation and relating to the individual*' includes the process by which the employee record is obtained or created;

(d) whether an employee's refusal to provide consent to the collection of sensitive 'information about an individual' in APP 3.3 is a breach of the respondent's Site Attendance Policy; and

(e) whether the 'consent' required by APP 3.3 includes 'implied consent', in circumstances where the employees have registered their fingerprint algorithm to be used by the scanners without first having been notified as required under the *Privacy Act*.

(2) Further, this case is the first occasion the Full Bench of the Commission has considered the essential question posed by the Commissioner's Decision; namely, whether the refusal of an employee to provide their biometric data through the scanning of fingerprints for the purposes of recording a person's presence at the workplace, constitutes a valid reason for dismissal, pursuant to the s 387(a) of the Act. We are satisfied that the appeal raises important, novel and emerging issues, not previously the subject of Full Bench consideration or guidance.

[36] For these reasons, we consider the public interest is enlivened by this appeal and we propose to grant permission to appeal. We order accordingly.

[37] The parties will be shortly advised concerning the hearing of the substantive appeal and the directions to be issued in preparation for the hearing.

DEPUTY PRESIDENT

Appearances:

J Lee for himself.
A Herbert of Counsel for the respondent.

Hearing details:

2018.
Sydney:
December 11.

Printed by authority of the Commonwealth Government Printer

<PR703676>