FairWork Commission

DECISION

Fair Work Act 2009
s.394 - Application for unfair dismissal remedy

Mr Jeremy Lee

v

Superior Wood Pty Ltd T/A Superior Wood
(U2018/2253)

COMMISSIONER HUNT BRISBANE, 1 NOVEMBER 2018

Application for an unfair dismissal remedy – dismissed after failing to comply with site attendance policy – refused to use biometric fingerprint scanners to record site attendance – no consent given by employee to collection of sensitive information – site attendance policy reasonably necessary for employer's payroll and safety functions - employee refused to follow lawful workplace policy – employee given multiple warnings and opportunities to follow site attendance policy - dismissal not harsh, unjust or unreasonable

[1] Mr Jeremy Lee was employed by Superior Wood Pty Ltd T/A Superior Wood (Superior Wood) from on or about 19 November 2014 to 12 February 2018. On 5 March 2018 Mr Lee made an application for a remedy for unfair dismissal under s.394 of the *Fair Work Act 2009* (the Act) alleging that he was dismissed from his employment on 12 February 2018 and that his dismissal was harsh, unjust or unreasonable.

Background

[2] Superior Wood operates sawmills on two sites at Melawondi and Imbil, Queensland. Mr Lee worked at the Imbil site at the time of his dismissal. Throughout his employment and at the time of his dismissal, Mr Lee was employed by Superior Wood as a general factory hand on a casual basis. Mr Lee's duties included the operation of forklifts and other machinery as well as the completion of other general tasks involved in the process of milling and processing timber. Mr Lee had originally worked from the Melawondi site, but was working from the Imbil site at the time of his dismissal.

[3] Superior Wood is part of the Finlayson Group of companies which handles wood products from plantation forest resource, through to processing and manufacturing, and product distribution.

[4] In October 2017 Superior Wood announced that it was introducing biometric scanners at the Imbil site for registering employee attendance and tracking shift times (the scanners). It was announced that 'all employees must use the biometric scanners to record attendance on site'.[1]

[5] Mr Lee objected to the use of the scanners and refused to use them in the course of his employment, as he was concerned about the collection and storage of his personal information by the scanners and Superior Wood.

[6] Between November 2017 and February 2018, Mr Lee and several managers of Superior Wood discussed Mr Lee's refusal to use the scanners. The parties were unable to resolve Mr Lee's concerns about the scanners and the employer's insistence that the scanners be used by all employees. On 12 February 2018, Mr Lee was issued with a letter of termination dismissing him from his employment on the grounds that he had failed to adhere to Superior Wood's Site Attendance Policy.

Relevant legislation

[7] Pursuant to s.385 of the Act, "*unfair dismissal*" is defined as meaning:

> "**385 What is an unfair dismissal**
>
> A person has been unfairly dismissed if the FWC is satisfied that:
>
> (a) the person has been dismissed; and
>
> (b) the dismissal was harsh, unjust or unreasonable; and
>
> (c) the dismissal was not consistent with the Small Business Fair Dismissal Code; and
>
> (d) the dismissal was not a case of genuine redundancy.
>
> Note: For the definition of consistent with the Small Business Fair Dismissal Code: see section 388."

[8] Further, s.387 relevantly provides:

> "**387 Criteria for considering harshness etc**.
>
> In considering whether it is satisfied that a dismissal was harsh, unjust or unreasonable, the FWC must take into account:
>
> (a) whether there was a valid reason for the dismissal related to the person's capacity or conduct (including its effect on the safety and welfare of other employees); and
>
> (b) whether the person was notified of that reason; and
>
> (c) whether the person was given an opportunity to respond to any reason related to the capacity or conduct of the person; and
>
> (d) any unreasonable refusal by the employer to allow the person to have a support person present to assist at any discussions relating to dismissal; and

(e) if the dismissal related to unsatisfactory performance by the person—whether the person had been warned about that unsatisfactory performance before the dismissal; and

(f) the degree to which the size of the employer's enterprise would be likely to impact on the procedures followed in effecting the dismissal; and

(g) the degree to which the absence of dedicated human resource management specialists or expertise in the enterprise would be likely to impact on the procedures followed in effecting the dismissal; and

(h) any other matters that the FWC considers relevant."

Capacity to bring application

[9] It is uncontested that Superior Wood dismissed Mr Lee from his employment by provision of the letter of termination on 12 February 2018. I am satisfied that Mr Lee was dismissed from his employment at the initiative of Superior Wood.

[10] Mr Lee's application was brought within the 21-day time period required by s.394(2) of the Act following his dismissal.

[11] Mr Lee was employed by Superior Wood as a regular and systematic casual employee. It is not contested and I so determine that he had a reasonable expectation of continuing employment with Superior Wood on a regular and systematic basis.[2] Me Lee's annual earnings were less than the high-income threshold amount. Mr Lee is protected from unfair dismissal under s.382 of the Act.

[12] Superior Wood is not a small business employer and is not subject to the Small Business Fair Dismissal Code.

[13] Mr Lee did not contend that his dismissal was a non-genuine redundancy.

[14] Therefore, the sole issue to be determined in this matter is whether Mr Lee's dismissal was an unfair dismissal pursuant to s.385 of the Act.

Conduct of the matter

[15] This matter was heard before me on 15 June 2018. Leave was granted for the parties to be represented. Mr Charles Martin of Counsel appeared for Mr Lee, instructed by the Caxton Legal Centre. Mr Andrew Herbert of Counsel appeared for Superior Wood, instructed by DWF Australia.

[16] The following people gave evidence. Mr Todd was not required for cross-examination:

- Mr Lee
- Mr Andrew Douglass, Director of Mitrefinch (Australia) Pty Ltd
- Mr Bruce Todd, Production Supervisor, Superior Wood Pty Ltd
- Mr Ian Swinbourne, Manager, Superior Wood Pty Ltd

- Mr Michael Lithgow, Technical Services Manager, Superior Wood Pty Ltd
- Mr Skene Finlayson, Director and Secretary, Superior Wood Pty Ltd

[17] Following the above hearing, and with leave, Superior Wood filed a second statement by Mr Finlayson. A second hearing was conducted on 10 August 2018 to allow for further cross-examination of Mr Finlayson.

Evidence of Mr Jeremy Lee

[18] Mr Lee's evidence was that he commenced employment with Superior Wood in November 2014 on a casual basis in the role of a general factory hand. Mr Lee had worked at Superior Wood's Melawondi site for approximately six months before transferring to the Imbil site, from which he had worked until the termination of his employment. Prior to October 2017, Mr Lee had been happy in his role and had been recognised for his good performance.

[19] Mr Lee stated that he and the other staff present at the Imbil site learned of the intention to install fingerprint scanners at a 'floor meeting' held at the Imbil site at 5:15am on 25 October 2017. A conversation to the following effect took place:

> Todd: A fingerprint scanner is being introduced for registering staff attendance. Over the next week you'll have to register your fingerprint. Michael Lithgow from administration is responsible for ticking off staff to make sure everybody registers. The scanner is going to be located on the outside of the administration building. Staff will be required to register attendance using the biometric scanner at the start and finish of shift.
>
> The scanner won't actually take a fingerprint.
>
> Lee: Yes it will.
>
> Todd: No it won't. The scanner uses an algorithm. It's not actually storing or keeping the fingerprint.
>
> Lee: It's scanning your finger, of course it's taking a fingerprint.
>
> Todd: I don't want to argue.

[20] Mr Lee stated that Mr Todd did not provide any explanation about why the scanners were being introduced. He considered that there was no consultation with employees about the introduction of the scanners, nor did the employer seek to secure the consent of employees to obtain biometric data. Employees were not provided with any written information or asked to read and sign any document.

[21] On 1 November 2017 Mr Lee was working at the Imbil site when he was approached by Mr Steve Howe, Floor Manager. Mr Howe directed Mr Lee to meet with Mr Lithgow to register his fingerprints for using the scanners.

[22] Mr Lee met with Mr Lithgow. The following was said:

Lee: I'm not comfortable providing my fingerprints to the scanner so I won't be doing it at this stage.

Lithgow: Everyone has to do it.

Lee: I understand your point of view. I am happy to discuss my concerns with Ian (Swinbourne) or Skene (Finlayson).

[23] Mr Lee did not provide his fingerprint to Mr Lithgow on 1 November 2017.

[24] On 2 November 2017 Mr Lee was directed to attend a meeting with Mr Swinbourne and Mr Finlayson. Mr Finlayson explained to Mr Lee several reasons why the scanners were being introduced in the workplace, including allowing the employer to streamline payroll and keep a track of people on site. Mr Finlayson said it was important for health and safety reasons.

[25] Mr Finlayson explained that he had considered other systems such as swipe cards, but he had chosen the scanner because there had been trouble in the past when staff could use a swipe card to swipe in for their 'buddies'.

[26] Mr Lee said to Mr Swinbourne and Mr Finlayson that he remained concerned about the control of his biometric data, and considered that Superior Wood could not guarantee that third parties would not access and use that data once it was stored electronically.

[27] Mr Finlayson said to him words to the effect, *"We are going ahead with this…hopefully Ian can address your concerns."* Mr Swinbourne said to him words to the effect, *"You have a decision to make."*

[28] Following the meetings of 1 and 2 November 2017, Mr Lee continued to use a physical 'sign in and sign out book' located in the Imbil site's administration office to record his attendance.

[29] On 7 November 2017 Mr Lee wrote to Mr Swinbourne detailing his concerns about the scanners and the collection of his biometric data. Mr Lee's letter stated:

> *"I am unwilling to consent to have my fingerprints scanned because I regard my biometric data as personal and private.*
>
> *If I were to submit to a fingerprint scan timeclock, I would be allowing:*
>
> - *Unknown individuals and groups to access my biometric data,*
> - *The potential trading/acquisition of my biometric data by unknown individuals and groups, indefinitely.*
>
> *Brief explanation:*
>
> *Information technology companies gather as much information/data on people as they can. Whether they admit to it or not. (see Edward Snowden)*
> *Such information is used as currency between corporations.*

All the largest technology companies – such as Apple, Google, Facebook, Telstra, Samsung – are in a race to access and store as much data on individuals as they can. This info is then traded and exchanged.

So if I were to consent to a fingerprint scan, my fingerprint would be scanned and stored for use immediately (regardless of assertions to the contrary), or it would be scanned and stored for use at a later time.

Jeremy Lee"

[30] On 22 November 2017 Mr Lee received a letter from Mr Swinbourne responding to his letter of 7 November 2017. Mr Swinbourne's letter stated:

"I would like to address your concerns re the implementation of Biometric scanning for payroll purposes. As you know the company has embarked on this common method to improve efficiency and accuracy of our payroll for approx. 400 employees.
You have raised some concern relating to your fingerprint security and use by others. I wish to outline some of the facts to help you make a decision on your own security concerns.

I have included a document from the supplier which outlines

- *The information gathered is not a finger print but a set of data measurements which is processed via an algorithm.*
- *There is no possible way the data measurements can be converted or used as a finger print.*
- *The company and its supplier cannot use your data measurements for any other purpose other than linking your payroll number to a clock in/out time.*

I trust this will address your concerns over the process."

[31] Mr Swinbourne's letter of 22 November 2017 attached a document explaining that the scanners did not collect an entire fingerprint, but determined 'unique points on a fingertip…to form a template which is a set of numbers…this biometric template cannot be used to re-create a fingerprint for identification purposes'.

[32] Mr Lee considered that Mr Swinbourne's letter did not address all of his concerns, and he remained concerned about the use of the scanners and the collection of his biometric data after 22 November 2017. Mr Lee continued to avoid using the scanners in the course of his employment after 22 November 2017.

[33] Mr Lee gave evidence that he was directed to attend several further meetings with Mr Swinbourne throughout December 2017. Mr Lee stated that at each of those meetings Mr Swinbourne detailed to Mr Lee the occasions on which he had attended the Imbil site in the course of his employment and not used the scanners. Mr Lee recalled that Mr Swinbourne, in each of the meetings said words to the effect, *"I urge you to start using the fingerprint scanner…it is not taking your fingerprint."* On one occasion he said, *"Even I have to use it."*

[34] On 9 January 2018 Mr Lee met with Mr Swinbourne and was given a verbal warning for refusing to use the fingerprint scanner. Mr Lee said to Mr Swinbourne words to the effect,

"The scanners can be cheated using fake fingerprints." He then asked what consequences may result from refusing to use the scanners, to which Mr Swinbourne replied words to the effect, *"That's a decision for you to make."*

[35] On 11 January 2018 he was directed to attend a meeting with Mr Swinbourne and Mr Howe. Mr Lee confirmed that he had not changed his mind about using the scanners, to which Mr Swinbourne responded by reading aloud and presenting to Mr Lee a written warning letter (the first written warning), which stated:

> *"The company has a strict policy on recording site attendance using Biometric Scanners. The system is used to both record attendance on site for Workplace Health and Safety and Payroll reasons.*
>
> *Up until the 2nd January 2018, the Biometric scanners have been in a trial mode to allow all employees to register and gain familiarity using the system. After an extensive trial period of seven weeks, a policy was issued on the 21st of December 2017 requiring all employees to record site attendance using the Biometric Scanner from the 2nd January 2018. This is the Site Attendance Policy.*
>
> *Throughout the trial period you have refused to register and use the system. You sighted [sic] concerns over giving up your own biometric data during this process. The Company has addressed these concerns as far as practicable by supplying the relevant information.*
>
> *During numerous discussions and meetings re the live implementation of the system, you have continued to refuse using the system.*
>
> *Your first rostered day back was 8th January and you made no attempt to register or scan. On the 9th, 10th, 11th of January you have made no attempt to register or sign in.*
>
> *On the 9th January you were issued with a verbal warning in relation to your refusal to register or sign in. It was clearly stated that you must follow the Site Attendance Policy.*
>
> *This is a written warning for failure to follow the Site Attendance Policy. Further failure to rectify this will result in a Final Written Warning. Continuing to not adhere to the Site Attendance Policy may result in your termination."*

[36] It was Mr Lee's evidence that he considered that he had, in fact, 'signed in' upon attending the Imbil site, using the physical sign-in book located in the Imbil site's administration office. Mr Lee continued to use the physical sign-in book to sign in and not the scanners after receiving the first written warning.

[37] On 17 January 2018 he was directed to attend a meeting with Mr Swinbourne and Mr Todd, during which Mr Swinbourne read aloud and presented to Mr Lee another written warning (the final written warning), which stated:

> *"Further to the Written Warning issued on the 11/1/18 re: failure to register and scan your attendance on site.*

On the 15th and 16th of January you have failed to register with the Biometric Scanner and scan your attendance with Superior Wood. This continues to be in breach of the Site Attendance Policy.

This is a Final Written Warning for failure to follow the Site Attendance Policy. I urge you in the strongest terms to comply with this Site Policy immediately. Further failure to comply with this will result in a Termination."

[38] On 18 January 2018 Mr Lee wrote to Mr Swinbourne in an attempt to resolve his concerns about the use of the scanners and the employer's insistence on mandatory use of the scanners. Mr Lee's letter stated:

"I value my job a great deal and your records will show that I have not missed a single day at work in over three years.

I have never given Superior Wood consent to scan my fingerprints or take my biometric data. I am hoping that by explaining my reasons more fully, there will be a satisfactory resolution allowing me to keep my job and my private biometric data.

- *The first time I was told about the installation of a fingerprint scanner was on Wednesday 25th October last year, at the start of the days [sic] shift (5.15am). At that time, the floor manager Bruce informed staff that Superior would be installing a "fingerprint scanner" and over the next week we would have to register our fingerprint for the system. He said that these scanners "don't take a fingerprint" and I immediately objected and said "Yes they do."*

- *On Wednesday 1sth November 2017 floor manager Steve Howe asked me to go down to see Michael Lithgow to register my fingerprints. I went straight to see Michael Lithgow and declined to scan my fingerprints and returned to work.*

- *On Thursday 2nd November, 2017 I had a meeting with Skeen Findlayson [sic] and Ian Swinbourne. It was explained to me that the system was being installed and I had to use it. Ian said I had "a decision to make". I was not asked for my consent.*

- *On Thursday 9th November, 2017 I gave Ian my letter refusing to give my consent to have my fingerprints scanned.*

- *On Wednesday 22nd November, 2017 Ian gave me a written reply to my letter while I was working.*

- *After my letter, during November and December 2017 I was approached several times by Ian to see if I had changed my mind. I told him no each time.*

- *On Tuesday 9th January, 2018 I had a meeting with Ian who gave me a verbal warning for refusing to use the fingerprint scanner. I asked for more information about the process "what happens from here" and was told "well that's a decision for you to make" but it was not explained to me further.*

- *On Thursday 11th January, 2018 Ian gave me a written warning at the end of the day.*

- *On Wednesday 17th January, 2018 Ian gave me a final written warning.*

During this whole time I have continued to use the sign in book as usual.

I understand managements [sic] need to account for employees [sic] work hours and would be happy to use any possible alternatives to sign in without providing my biometric data. I could continue to time in/out using the sign-in book, or I could use an employee number, or a password, or a timecard, etc.

From the 25th November forward I have been told that I must use the fingerprint scanner, or be sacked. No alternative has been offered.

Staff were told "You have to do it, there is no option".

Superior Wood did not seek consent from staff. There was no consultation with staff. The system was simply installed and staff were informed they were to use it.

Superior Wood has given me nothing to sign to give my consent or provide assurances of how, when, where, who could access my data. There was not any acknowledgement of privacy, no privacy statement or data handling statement or mention of the companies' [sic] privacy obligations.

I would love to continue to work for Superior Wood as it is a good, reliable place to work. However, I do not consent to my biometric data being taken.

The reason for writing this letter is to impress upon you that I am in earnest and hope there is a way we can negotiate a satisfactory outcome."

[39] Mr Lee stated that the next discussion he had with Superior Wood about the scanners was during a meeting on 24 January 2018 that he attended, along with Mr Swinbourne and Mr Finlayson. Mr Bill Gethin also attended the meeting as Mr Lee's witness and support person. Mr Lee stated that Mr Finlayson began the meeting by reading aloud Mr Lee's letter of 18 January 2018. Mr Finlayson then asked Mr Lee whether he would use the scanner, to which Mr Lee responded, *"No."*

[40] Mr Finlayson said to Mr Lee words to the effect, *"You have to use the scanner…it allows us to keep a better track of where people are…if someone gets injured on site I could be sued for twenty million dollars."* Mr Finlayson referred to the information document provided to Mr Lee on 22 November 2018 and reiterated that the scanners did not record a fingerprint.

[41] Mr Lee responded to Mr Finlayson words to the effect, *"The scanner still relies on trust because someone could scan in in the morning and then come back in the afternoon and scan out."* Mr Lee said further that the information document previously provided to him did not address his concerns about the collection of his 'biometric data', and he did not consent to anyone collecting his biometric data.

[42] On 30 January 2018 he was directed to attend a meeting with Mr Swinbourne and Mr Todd. During that meeting Mr Swinbourne noted to Mr Lee that he had received several

warnings about using the scanners and directed Mr Lee to use the scanners. Mr Lee agreed that he had been given several opportunities to reconsider using the scanners, but did not agree to use the scanners.

[43] Mr Lee stated that Mr Swinbourne said *"[you are]…required to show cause why further action should not be taken"*, to which Mr Lee responded, *"I believe my two letters have shown cause but if you can point to something that you do not understand or don't agree with I would be happy to try to explain it better."*

[44] On 6 February 2018 he was directed to attend a meeting with Mr Swinbourne and Mr Todd to show cause as to why his employment should not be terminated. Mr Lee reiterated that he had explained his reservations about using the scanners in his two previous letters. Mr Swinbourne informed Mr Lee that he would discuss the matter with Mr Finlayson, who would make a decision.

[45] On 12 February 2018 he was directed to attend a meeting with Mr Swinbourne and Mr Howe. At the start of the meeting Mr Lee confirmed that he still refused to use the scanners in the course of his employment. Following Mr Lee's confirmation, Mr Swinbourne read aloud a letter addressed to Mr Lee, terminating his employment with Superior Wood effective immediately (the Termination Letter). Mr Swinbourne presented a copy of the Termination Letter to Mr Lee, which stated:

> *"RE: Failure to adhere to Site Attendance Policy.*
>
> *The Site Attendance Policy clearly states that you must sign into site using the biometric scanners provided. A trial period of seven weeks enabling all employees to gain an understanding of the system function has occurred. This was completed on the 21st Dec 2017. Information prior to and during this trial period has been given to employees.*
>
> *Thus far you have not registered and scanned for your attendance on site and this is in clear breach of this policy. During the trial period you showed reservations to registering and scanning for your attendance. You addressed a letter to the company on the 7th November requesting further information and listing your reasons for not taking part in the process. The company responded to questions with a letter and documents addressing your concerns.*
>
> *The following warnings and discussions have taken place since 21st December 2017 in relation to breaching the Company Site Attendance Policy*
>
> - *Verbal Warning 9/1/18*
> - *Written Warning 11/1/18*
> - *Final Written Warning 17/1/18*
>
> *Despite the warnings above you continued to fail to adhere to the Site Attendance Policy.*
>
> *Meeting with the Company Director, Superior Wood Manager and yourself, with Bill Gethin Jones as your witness – 24/1/18*

- *The company reinforced its requirement to adhere to the lawful and reasonable instruction in the Site Attendance Policy. It is a strict WH&S requirement in addition to payroll functionality.*
- *The company reiterated the information given in relation to the use of biometrics. Specifically referring to the system not gathering a finger print.*
- *You continue to refuse to follow the Site Attendance Policy.*

Further meeting with Superior Wood Manager, Dry Mill Supervisor, and an offered witness (not taken) – 30/1/18

- *The company again reinforced its requirement to adhere to the Site Attendance Policy.*
- *You stated there was no change in refusal to adhere to the Policy.*
- *The company has given you all information required on the Biometric Scanner.*
- *The company reinforces that Jeremy has been given sufficient notice, sufficient trial period and a verbal, written and final written warning.*
- *The company requested a letter from Jeremy to show cause why further disciplinary action should not be taken.*

Further meeting with Superior Wood Manager, Dry Mill Supervisor, and an offered witness (not taken) – 6/2/18

- *Company reiterated again the requirements of the Site Attendance Policy*
- *Jeremy states he will not follow this Policy*
- *Jeremy cannot provide a show cause letter as requested in the previous meeting*
- *Jeremy refers back to his original letter and states that this is his show cause letter*
- *Meeting ended with no further discussion.*

Despite the numerous discussions, warnings and information provided back to yourself, you have continuously refused to adhere to the Site Attendance Policy. The company has met all requests for information to enable you to successfully follow the Site Attendance Policy.

Due to the above events you are given notice of your termination, effective immediately. Two weeks notice will be paid into your account.

Date: 12/2/18

Ian Swinbourne
Manager
Superior Wood"

[46] In cross-examination, Mr Lee was asked if it was a condition of going back to work, would he provide his biometric data? He answered that he would not provide his biometric data.[3]

[47] Mr Lee agreed that the alternatives put on his behalf, such as a swipe pass or password can be falsified by others. It was Mr Lee's evidence that if he were to return to the workplace his preference would be to continue to sign-in using the paper sign-in book at reception. When informed that Superior Wood no longer uses the paper sign-in book, Mr Lee responded that he was not aware of that.[4]

[48] The following exchange occurred:[5]

> Mr Herbert: So it's because you object to giving out your biometric data you should be treated by the company as being exempt from the security measure that they've introduced. Is that what you're telling the Commission?
>
> Mr Lee: Exempt from the security measure. Yes, I didn't think about it that way. I just think that my biometric data is mine and I didn't want to give it away and have someone else control it and have it.

[49] Mr Lee agreed that he has a driver's licence, and has provided his biometric data to the Queensland transport department in the form of his driver's licence photo. Likewise, he has a passport, and he understands that facial recognition software is used for people going in and out of Australia by the relevant departments responsible for immigration and counter-terrorism.

[50] Relevant to Mr Lee's understanding or belief that a fingerprint would not be obtained if he were to use the fingerprint scanner, the following exchange occurred:[6]

> Mr Herbert: Just on that - I won't take very long, Mr Lee, but just on that, you understand that what happens is that the scanner takes various dot points of interest from your fingerprint and it converts all that into an electronic message and is processed by a complicated algorithm so that it can be readily compared to the next time that fingerprint is placed on the scanner. You understand how that works, in general terms?
>
> Mr Lee: Yes.
>
> Mr Herbert: You understand also that it doesn't actually take a photograph or anything like that of a fingerprint and that a fingerprint cannot be created out of the data that it takes. You can't recreate a fingerprint out of that data, because it's got dots, and the lines between the dots are not recorded. Do you accept that? That's what you've been told?
>
> Mr Lee: Yes, I've been told that; yes.
>
> Mr Herbert: Do you accept it?
>
> Mr Lee: No.
>
> Mr Herbert Why? Do you have any evidence that that's untrue, or is it just in your mind you don't agree with it?

Mr Lee: Yes there's in general evidence everywhere.

…

Mr Herbert: Sorry?

Mr Lee: Yes, in general there's evidence everywhere in the information technology sector that they are keeping more than they let on, they are using it in different ways than they let on and, yes, my view of that explanation of the fingerprint scanner is - it's a palatable explanation of what they do with it, and it's actually worse, I think, that they most probably do take a fingerprint scan and can recreate a fingerprint, but most people won't see that. That will - most people won't, yes. It's not accessible by most people.

Mr Herbert: You obviously have brought no evidence to this Commission to establish that what the provider of that machine says is not true, because you understand - for example, you've seen the evidence of Mr Douglass where he says you cannot create a fingerprint from the data that's collected. You have no evidence that what he says is not true, have you?

Mr Lee: No, I'm not presenting any evidence that that's not true.

[51] In a later exchange, Mr Lee was asked his concern as to having his fingerprint reconstructed. The following was put to him and answered by him:[7]

Mr Herbert: No, and what is it that you think would be the value to anyone of biometric data constituted by some points taken from one of your fingerprints? What do you think someone could conceivably do with that information anyway, even if it was to be trafficked, as you say?

Mr Lee: There's kind of similar things that people do with - say if someone steals a wallet, they've got stuff they can make up an identity, put me somewhere that I'm not.

Mr Herbert: Put you somewhere you're not?

Mr Lee: Yes.

Mr Herbert: You think somebody might reconstruct a fingerprint out of this data, even though you were told it can't be done, and then create a false fingerprint and then put your fingerprint somewhere where you weren't. Is that what you think might happen?

Mr Lee: It's conceivable.

Mr Herbert: Why do you think anybody on the face of planet earth would do a thing like that to you?

Mr Lee: It's like - it's valuable data that companies, and information companies, are seeking to get, so…

Mr Herbert: To do what? What can they do? It's not your shopping habits, it's not your likes and dislikes with sports or movies?

Mr Lee: It's empowering. It's empowering to those that have it.

Mr Herbert: How does it empower them? What power do they have over anybody by having a reconstructed fingerprint of yours?

Mr Lee: The power of surveillance and - it's a bit hard to describe. It's like you have - it's kind of like ownership. You can surveil them. You own their biometric data. I mean, it's…

Mr Herbert: You own their biometric data and you can use your ownership of a fingerprint to surveil a person. Have you joined those dots together? Perhaps you can explain how those things fit together. How does getting access to an algorithm which records points on a person's fingerprint give that person who's got that algorithm or that material the ability to surveil you?

Mr Lee: If you reconstitute to a fingerprint that's usable by people from - visually, so that's more useful, and also you don't have to reconstitute it into a fingerprint for it to be - it's a biometric template as it is.

Mr Herbert: How do people get to surveil you as a result of that?

Mr Lee: They don't get to surveil you with your fingerprint, but it's part of my biometric data. It's my identity, and if they take it it's empowering to them.

Mr Herbert: You've already empowered all the people that you've given your photograph to in all sorts of high places in government, haven't you?

Mr Lee: Yes, I have.

Mr Herbert: And you're going to draw the line?

Mr Lee: And I dislike it.

Mr Herbert: Yes, and you're going to draw the line with this company. Is that your position?

Mr Lee: It's not really Superior that I object to taking it, it would be anyone.

[52] Relevant to health and safety risks in a large sawmill, Mr Lee agreed that there are lots of combustible materials within the mill, and a high risk of fire. He agreed that people can become trapped.[8] He agreed the employer would need to know in the event of an emergency if anybody was trapped, and if all people on site had evacuated safely.[9]

[53] Relevant to the payroll system and the improvements that the employer would achieve in having biometric scanning, Mr Lee speculated that people might be able to use 'dummy fingers', for example, a prosthetic or rubber finger. He was unsure if a person might be able to use a dummy fingerprint to abuse the system.[10]

[54] In answering questions from me, Mr Lee confirmed that Superior Wood has a drug and alcohol policy. While he was never obligated to provide a sample, Mr Lee's understanding is that it required an employee to provide a urine sample. He agreed that if had been required to undertake a test, he would have done so.[11]

[55] In the scenario where Mr Lee would have provided a urine sample, and it had been sent to a pathology laboratory for further testing, Mr Lee stated that he would be 'OK' with that scenario. He said, *"I wouldn't regard the pathology lab testing urine as risky, I would say."*[12]

[56] I put the following to Mr Lee and he answered as follows:[13]

Commissioner: Aren't they more easy - in a better position, if you have any concerns about somebody pretending you're somewhere where you're not, wouldn't it be easier to obtain a small sample of the urine that you had provided for testing and putting you in that place than it is for somebody to reconstruct a fingerprint?

Mr Lee: Yes. Potentially, yes.

Commissioner: So you would trust that pathology and you don't trust this organisation?

Mr Lee: Yes, I would be more inclined to trust pathology; yes. It depends. I guess if the pathology worked with police, had police contracts, I might be a bit concerned.

Commissioner: You'd be worried, would you, if the pathology organisation worked with police, because of - why?

Mr Lee: It has happened in the past, because - in the UK, that pathology labs were leaned on to get results for police in cases. So it's like they want to please the police.

Commissioner: Your evidence earlier was that up until today, if you had have been required to undertake a urine, drug and alcohol test you would have done so at the workplace?

Mr Lee: Yes.

[57] Regarding mitigation, Mr Lee stated that he has been attempting to obtain work, but has been unsuccessful. He stated that he had applied to Coles, IGA, Woolworths, Laminex, rendering and roofing businesses, an auction business, factory positions in Gympie and also to some employers in Brisbane. He had received some calls, but had not secured interviews.

[58] In answering my questions during the hearing, Mr Lee stated that he recently objected to an application with Coles because Coles required a psychological profile on his application and he objected to it. Mr Lee agreed that he would decline work if it was in a workplace where biometric scanning was required, or the employer required psychometric testing as pre-employment criteria.

Evidence of Mr Ian Swinbourne

[59] Mr Ian Swinbourne is the Manager of Superior Wood and has been employed by Superior Wood for approximately 24 years. He was responsible for the management of Mr Lee's employment during the relevant period of time in this matter.

[60] Prior to the implementation of the scanners at the Imbil site, manual time sheets were used by employees who were required to sign in and sign out by writing in the relevant time and adding their signature.

[61] Mr Swinbourne confirmed that the trial period for the scanners was for seven weeks starting in early November 2017. Employees were gradually enrolled into the system during this time while manual time sheets were still available for use. A pamphlet explaining the scanner was provided to employees and also made available on notice boards in the lunch room and near the scanner itself.

[62] Mr Swinbourne conceded that at the relevant time Superior Wood did not have a privacy policy to cover employees; the one-page privacy policy admitted into evidence was only relevant to the information obtained by persons accessing the Superior Wood website.

[63] On 2 January 2018 an updated Site Attendance Policy was introduced. It was posted near the scanner for all employees to read. The Site Attendance Policy reads:

> *"Site Attendance Policy*
>
> *Due to company Workplace Health and Safety and Payroll requirements it is imperative all employees are accounted for on site.*
>
> *Therefore as at the 2nd January 2018 it is policy that all employees must use the biometric scanners to record attendance on site.*
>
> *It is reinforced that the biometric scanners do not take a finger print. The algorithm data used to record attendance cannot be used to generate a fingerprint.*
>
> *Please ensure you scan in when arriving on site and leaving site at the end of your shift. If you are having issues with scanning please see your supervisor. If you fail to use or attempt to use the biometric scanner then disciplinary action may be taken. Signing the attendance sheets alone is no longer acceptable.*
>
> *The Directors and Superior Wood Leadership would like to thank employees for their assistance and patience during the 'trial' period."*

[64] Relevant to the meetings involving Mr Swinbourne and Mr Lee on 2 November 2017 and 9 January 2018 as referred to at paragraphs [24] – [27] and [34] Mr Swinbourne denies that he ever said to Mr Lee words to the effect, *"You have a decision to make"* in relation to use of the scanners.

[65] Mr Swinbourne confirmed that two written warning letters were provided to Mr Lee on 11 January 2018 and 17 January 2018. Mr Lee was offered a support person at all meetings where the Site Attendance Policy was discussed.

[66] Mr Swinbourne considered that had Mr Lee's employment continued, the alternatives open to Superior Wood regarding Mr Lee signing in and out would have been:

- Allow Mr Lee to use manual time sheets – Mr Swinbourne stated that this would have left Superior Wood open to time recording inaccuracy and fraud which the scanner was designed to prevent;
- Allow Mr Lee to use a surgical glove when using the scanner – Mr Swinbourne stated Superior Wood would have accommodated this because the scanner can still operate through a surgical glove;
- Allow Mr Lee to use an artificial fingerprint, not his own fingerprint – Mr Swinbourne stated that this would not have been appropriate because the artificial fingerprint could be used by other staff, defeating the purpose of the system.

[67] Mr Swinbourne stated further that pursuing alternative arrangements for Mr Lee to sign in and out would have been costly to Superior Wood.

[68] In any event, Mr Swinbourne stated that if Mr Lee was allowed to be exempt from using the scanner, it would be difficult to justify requiring any other staff who objected, with or without dishonest intent, to use the system.

[69] During the hearing Mr Swinbourne stated that for a period from early November 2017 up until around 1 June 2018, both the biometric scanning and the paper sign-on sheets had been used. Both systems were used by Superior Wood to allow for cross-checking the accuracy of the payroll to ensure the employees were correctly paid.[14]

[70] In cross-examination Mr Swinbourne agreed that there had been a fire alarm trigger at the site in January 2018. The paper sign-on book was used to determine the presence of employees.

[71] Mr Swinbourne agreed that he did not explore the possibility of using another system of time and attendance for Mr Lee given his objections. Mr Swinbourne stated that it was not within his scope or responsibility for the site.[15] He did not make inquiries as to how much other systems might have cost to implement.

[72] Mr Swinbourne agreed that he had not been issued with a collection notice under *The Privacy Act 1988* (Privacy Act) by either Superior Wood, Finlayson's Timber & Hardware Pty Ltd, Mitrefinch or by any other company in the Finlayson Group.

[73] In answering questions from me, Mr Swinbourne stated that Superior Wood has an employee on-site trained to conduct drug and alcohol testing using saliva. If an employee on-site produced a non-negative result, the employee is to be escorted by the employer and required to go to a general practitioner or pathology laboratory where a urine test will be conducted. A negative saliva sample on-site is destroyed on-site. A non-negative saliva sample provided on-site travels with the employee and the escort to the general practitioner or pathology laboratory.

[74] Mr Swinbourne agreed that the trained employee on-site is entrusted with the oral fluid samples of employees.

Evidence of Mr Skene Finlayson

[75] Mr Finlayson is the sole director and secretary of Superior Wood. Superior Wood has approximately 150 employees and is part of the Finlayson Group of companies, which has acquired a number of businesses over the last five years.

[76] Mr Finlayson said the Finlayson Group had found the payroll function was being conducted on three different days each week, resulting in a number of errors due to manual time-keeping systems. Mr Finlayson outlined the following issues the payroll department encountered with the manual time-keeping system:

- Staff signing into and out from work at the same time, when they arrived at work, so that there was no guarantee that their actual departure time matched the time they had filled in on arrival that day;
- Staff who arrived late inserting their normal start time rather than their actual arrival time;
- Staff signing in for another staff member when that staff member was late;
- Staff being paid when they were absent because of false timesheet entries; and
- Staff being paid incorrectly in relation to sick pay and annual leave.

[77] Mr Finlayson said a number of options were investigated by the payroll department to streamline the process. Mitrefinch was awarded the contract after the project was put to tender, due to three main factors:

- The Mitrefinch system was able to be fully integrated with the current operating system;
- The Mitrefinch system improved safety across all sites;
- The Mitrefinch system had installations in over 340 businesses operating in Australia, and 'thousands' worldwide.

[78] Mr Finlayson also stated that the scanner had been introduced across six other Finlayson Group sites over the preceding 18 months, involving around 400 employees. No other employees in the Finlayson Group had refused to use the scanner, and Superior Wood was the last company in the Finlayson Group where the scanner was rolled out. The introduction of a new time and attendance system was discussed at a biannual company update conducted on 27 June 2017. The scanner was installed at the site well before it was actually used.

[79] Mr Finlayson stated that on account of the biometric scanning, the above payroll issues had been eliminated, with the added bonus that supervisors could now quickly download who is on any site at any given time. Mr Finlayson stated he regarded this function as a very important part of the company discharging its work, health and safety obligations, for example, in the event of a premises evacuation. If a manual system continued to be used, if an employee had been falsely signed in when they were truly absent, in the event of an emergency, staff might be unnecessarily endangered mounting a search for an employee not present at work.

[80] Mr Finlayson stated that at the meeting of 2 November 2017 he told Mr Lee that the Mitrefinch system had been progressively rolled out in other companies in the Finlayson Group, and it was now time to implement the system at Superior Wood. Mr Finlayson stated

he also told Mr Lee that the scanner provided significant benefits in relation to workplace health and safety and that the system did not take a fingerprint, only an algorithm.

[81] Mr Finlayson denies hearing Mr Swinbourne say to Mr Lee the words, *"You have a decision to make"*, or that Mr Finlayson said to Mr Lee, *"Hopefully Ian can address your concerns."*

[82] Mr Finlayson stated further at the meeting of 24 January 2018 he discussed with Mr Lee the inaccuracies of the current manual time-recording system. Mr Finlayson said he recalled stating to the effect that he respected Mr Lee's decision not to use the scanner. Mr Finlayson denies saying, *"I could be sued for $20 million"*, but does recall saying he could be fined or imprisoned. Mr Finlayson also said he could not recall Mr Lee saying, *"That does not address my concerns"*.

[83] Mr Finlayson stated that it was his view that Mr Lee's employment with Superior Wood would not have continued for very long, because Mr Lee had shown an unwillingness to follow an important company policy. Mr Finlayson also stated that unless Mr Lee signed in via the scanner, a payment file could not be generated and therefore Mr Lee would not be paid by the payroll system.

[84] Mr Finlayson stated that he opposed reinstatement of Mr Lee on the grounds that he had lost faith that Mr Lee would act in the best interests of the company or follow directions and policies. Mr Finlayson also stated he had significant concerns about operating a different workplace health and safety and payroll system for one employee. Mr Finlayson also stated that the company is looking to downsize in an effort to compete with mouldings coming in from China.

[85] During the hearing Mr Finlayson gave evidence regarding the storage of data collected by the scanners. Mr Finlayson stated that the data collected by the scanners was stored off-site by a third-party information technology company, 'Oz IT', which also collected data from scanners used in other companies within the Finlayson Group of companies, similar to the scanners in use at Superior Wood.

[86] Mr Finlayson stated that the data collected by the scanners used within Superior Wood's workplaces was stored on servers owned by the Finlayson Group within an area leased on a monthly basis from Oz IT (the servers). Mr Finlayson stated that Oz IT and its staff would have access to the data stored on the servers owned by the Finlayson Group. Mr Finlayson stated that to his knowledge, Oz IT had a privacy policy in relation to the use of those servers.

[87] Mr Finlayson stated two employees of another company, the Finlayson Timber and Hardware Company, routinely accessed the data stored on those servers for the preparation of payroll for Superior Wood. Mr Finlayson stated that the only people with access to the data stored on the servers were the two employees of the Finlayson Timber and Hardware Company and the two 'working directors' of the Finlayson Group.

[88] Mr Finlayson reiterated his concerns about allowing Mr Lee to operate on a different payroll system and site attendance policy than the other employees of Superior Wood and within the Finlayson Group. Mr Finlayson stated that the nature of the sawmilling work conducted by Superior Wood was dangerous and it was his responsibility to ensure that his

employees were safe and the implementation of the scanners within Superior Wood provided an additional safety measure. Mr Finlayson stated that he had to make the choice to terminate Mr Lee's employment because he could not allow Mr Lee to be subject to different policies regarding site attendance and safety than the other employs of Superior Wood.

[89] In cross-examination Mr Finlayson agreed that there had been a number of fire alarms at Superior Wood during 2018, although he could not recall the exact dates. It was put to Mr Finlayson that during a fire alarm in January 2018, attendance of staff at the designated assembly point was checked by reference to the physical sign-in sheets and not by reference to the attendance information collected by the scanners. Mr Finlayson could not give evidence on the procedures followed during that fire alarm, as he had not been present on-site during the alarm.

[90] Mr Finlayson agreed that Superior Wood does not have a privacy policy reflecting the Australian Privacy Principles set out in the Privacy Act that governs the privacy of its employees.

[91] Mr Finlayson agreed that the servers are owned by the Finlayson Timber and Hardware Company, and that the data collected by the scanners in use within Superior Wood are stored on those servers. Mr Finlayson agreed that no notice or letter had ever been sent to any employee of Superior Wood disclosing that the data collected by the scanners is stored on servers owned by another company, being the Finlayson Timber and Hardware Company.

[92] Mr Finlayson confirmed that Mr Lee's employment, if it had not ended on 12 February 2018, would have ended a short time after as Mr Lee had demonstrated an unwillingness to follow the site attendance policy.

[93] Mr Finlayson stated that any other position with no less favourable terms and conditions of employment that Mr Lee may have been able to have been redeployed to in a company within the Finlayson Group would also have required Mr Lee to use a scanner in the course of his employment.

[94] Mr Finlayson accepted that Superior Wood could not lawfully require Mr Lee to provide certain kinds of information dealt with under the Privacy Act without his consent.

[95] In answering questions from me, Mr Finlayson stated that site attendance information produced from the data collected by the scanners could be accessed by supervising employees within Superior Wood. For example, the site attendance information could be downloaded or displayed on a supervisors' phone to show which employees were present on site at the relevant time.

[96] Mr Finlayson stated that before the introduction of the scanners, site attendance could only be confirmed by reference to the physical sign-in sheet located in the administration building within Superior Wood's worksites, which a supervisor would need to retrieve from the administration building.

[97] In Mr Finlayson's second statement he said that while the scanner used at Superior Wood was initially purchased by Finlayson Timber & Hardware Pty Ltd, at all relevant times, Superior Wood had sole possession and control of the scanner, and it was operated only by Superior Wood staff.

[98] For accounting purposes, Mr Finlayson stated that it is common practice for capital items to be purchased by Finlayson Timber & Hardware Pty Ltd, and transferred to other members of the Finlayson group of companies who may have need for it.

[99] There was no formal leasing arrangement documented for the transfer of the scanner to Superior Wood, however the scanner is treated for all purposes as having been transferred to Superior Wood by Finlayson Timber & Hardware Pty Ltd for the sole use by Superior Wood.

[100] Finlayson Timber & Hardware Pty Ltd charged and collected from Superior Wood an administration fee of $9,000 per month for various charges. An amount of $1,250 per month was charged within the $9,000 total for the purposes of the use by Superior Wood for the scanner placed at Superior Wood.

[101] Mr Finlayson agreed in his second statement that at the time of the dismissal, neither Superior Wood or Finlayson Timber & Hardware Pty Ltd had in place a Privacy or Confidentiality Policy. Policies have now been introduced.

[102] Relevant to the contractor providing IT hosting services on the server owned by Finlayson Timber & Hardware Pty Ltd, Mr Finlayson provided a copy of an unsigned agreement between Finlayson Timber & Hardware Pty Ltd and Aus IT Services Pty Ltd. Mr Finlayson stated that the parties have been meeting respective obligations pursuant to the unsigned agreement since 20 October 2016 as though it were signed. The agreement requires each party to meet its obligations under the Privacy Act. Mr Finlayson stated that the agreement applies to members of the Finlayson Group, including Superior Wood.

[103] Mr Finlayson attached to his second statement a copy of the Mitrefinch 'Data Loss Assessment and Reporting Procedure' adopted on 15 May 2018. It is a document generated from Mitrefinch's United Kingdom office and deals with actions taken if a data breach is identified.

Evidence of Mr Michael Lithgow

[104] Mr Lithgow has been the Technical Services Manager at Superior Wood since 2002. Mr Lithgow stated that his responsibilities include optimising the scanning system, computer systems maintenance and training, installation of new technologies as well as wood procurement and timber certification.

[105] Mr Lithgow stated that scanners had been present on site at Imbil and Melawondi from 2016, visible to employees before they were eventually installed around October 2017.

[106] Mr Lithgow stated he was responsible for registering 90% of the Imbil employees to the scanner in November and December 2017. Mr Lithgow explained the process as follows:

- An employee entered a number specific to them and scanned a finger (usually the index finger) three times;
- Another scan of that finger was then performed to verify the entry;
- This process was then repeated for the same finger on the other hand in case of injury.

[107] Mr Lithgow confirmed he had discussions with Mr Lee regarding the methodology and operation of the scanner on multiple occasions between November and December 2017. Mr Lithgow stated that he explained to Mr Lee that the scanner did not record fingerprints.

[108] Mr Lithgow also confirmed that Mr Lee's recollection of the events surrounding the floor meeting Mr Lee attended on 25 October 2017 at 5.15am and the subsequent conversation Mr Lee had with Mr Lithgow on 1 November 2017 was accurate.

[109] In cross-examination, Mr Lithgow stated that he had not received from Superior Wood a collection notice under the Privacy Act. Mr Lithgow stated further that he had not been informed on any occasion that any other entity besides Superior Wood had received his 'biometric template' or 'biometric information'. Mr Lithgow stated that he was not aware of where the 'biometric template' collected by the scanners was stored.

Evidence of Mr Andrew Douglass

[110] Mr Douglass is the director of Mitrefinch (Aust) Pty Ltd and has been working for the Mitrefinch group of companies for over 30 years. He has worked as a Systems Analyst, Programmer and IT and Implementation Manager in that time.

[111] Mr Douglass stated that he is currently responsible for the operation of Mitrefinch (Aust) Pty Ltd, and still performs some installations of Mitrefinch systems at client sites, as was his role as an Implementation Manager.

[112] The Mitrefinch scanner captures features of the tissue that lie below the skin as well as on the finger surface. The scanner uses a special algorithm to ascertain coordinates of the "minutiae" (numerous points on a finger) which are then stored as a series of numbers. Mr Douglass provided the Commission with an example of finger template data generated and stored by the scanner.

[113] Mr Douglass explained that the scanner does not store actual fingerprints or fingerprint image data and it is not possible to reconstruct a person's fingerprint from the template produced by the scan, as the scan does not retain enough detail of the skin patterns on the fingerprint. Further, a biometric reader is not able to use normal fingerprint images as the data involved is too large to store, and takes too long to process.

[114] Mr Douglass confirmed that the scanner was designed to operate through a tight-fitting medical glove and could also operate irrespective of calluses, dirt, moisture, wrinkles, contaminants, ink, glue or paint on the skin surface.

[115] Use of a scanner within a workplace ensures that only the employee can register or clock themselves in or out of a workplace, and the time that they do on each occasion is accurately recorded in real time. Mitrefinch has implemented over 500 scanner systems with employers throughout Australia and New Zealand in the last 16 years. Globally there are almost 1 million employees using the system.

[116] Mr Douglass stated that the Mitrefinch scanner uses Lumidigm multi-spectral imaging technology and that the algorithm used to ascertain the coordinates was proprietary to the manufacturers of the Lumidigm readers, such that it is not made known to equipment

managers such as Mitrefinch. Mitrefinch manufactures the registration terminal that houses the scanner; Mitrefinch installs the scanners into each terminal; however Mitrefinch does not manufacture the actual scanner.

[117] The customer contracted by Mitrefinch is Finlayson Group.

[118] Mitrefinch has remote access to the application installed on the Finlayson Group server to provide remote support when required by Finlayson Group. Mr Douglass stated that Mitrefinch did not provide this information to any external parties.

[119] The biometric template of each employee is stored firstly in the 'reader' of the registration terminal at the workplace, and a copy is kept in the Finlayson Group database server. Mr Douglass stated that the purpose of Finlayson Group storing the second copy at its offsite server is if an employee within the Finlayson Group is enrolled at one terminal on one site, and is required to go to another site, the employee does not have to go to each terminal and enrol individually on them. Additionally, if a terminal is replaced through faults, or for any other reason, the template stored on the server is provided to the site terminal, ensuring the employees do not have to be taken back to the site terminal to re-enrol.[16]

[120] Mr Douglass agreed that Mitrefinch has the ability to obtain the stored data on the Finlayson Group server, if it was necessary to do so. Mitrefinch has not, to-date, had any reason to do so, and might only ever need to in the event of a data corruption event. Mr Douglass confirmed that Mitrefinch has not ever required access to *any* client's storage of biometric data of its employees.

[121] In cross-examination Mr Douglass was asked if Mitrefinch has an Australian Privacy Principles (APP) policy. He stated that he did not know; he might need to refer to 'head office in the UK', and that he has not seen one.

[122] In answering questions from me, Mr Douglass stated that he was not familiar with the APP's. He stated that Mitrefinch has 14 employees in Australia, and nobody has a title that includes things such as 'Data Privacy Officer'. He stated, *"We are owned wholly by Mitrefinch Ltd in the UK. They tend to take care of these issues."*

Mr Lee's submissions

Australian Privacy Principles

[123] APP is a reference to the Australian Privacy Principles within the *Privacy Act 1988* (Privacy Act). It is asserted that Superior Wood does not contest that it is an APP entity within the Privacy Act.

[124] It is submitted that the sole reason for Mr Lee's dismissal was his failure to comply with Superior Wood's Site Attendance Policy and subsequent directions to obey it by refusing to use the biometric scanner to clock on and off. Mr Lee submits that this does not constitute a valid reason for the dismissal because neither the Site Attendance Policy nor the directions to comply with it were lawful.

[125] Mr Lee submitted that failure to comply with an unreasonable direction is not a valid reason for dismissal,[17] and an employee is only obliged to obey orders which are both lawful and reasonable.[18]

[126] It is submitted that the Site Attendance Policy and directions to comply with it were unlawful because they involved contravention of s 13G of the Privacy Act. Section 13G of the Privacy Act is produced below:

> **"13G Serious and repeated interferences with privacy**
>
> An entity contravenes this subsection if:
>
> (a) the entity does an act, or engages in a practice, that is a serious interference with the privacy of an individual; or
>
> (b) the entity repeatedly does an act, or engages in a practice, that is an interference with the privacy of one or more individuals.

[127] As to the definition of what 'interference with the privacy of an individual' means, it is defined in s.13 of the Privacy Act to mean:

> (1) An act or practice of an APP entity is an interference with the privacy of an individual if:
>
> (a) the act or practice breaches an Australian Privacy Principle in relation to personal information about the individual; or
>
> (b) the act or practice breaches a registered APP code that binds the entity in relation to personal information about the individual.

[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.

[130] The APP privacy policy must at least contain certain listed information, including how the entity collects and holds personal information, and the purposes for which the entity collects, holds, uses, and discloses personal information. Each entity must take reasonable steps to ensure that its APP privacy policy is freely available in an appropriate form.

[131] APP3 governs the collection of solicited information by APP entities. APP3 is produced below:

"3 Australian Privacy Principle 3--collection of solicited personal information

Personal information other than sensitive information

3.1 If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.

3.2 If an APP entity is an organisation, 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.

Sensitive information

3.3 An APP entity must not collect sensitive information about an individual unless:

(a) the individual consents to the collection of the information and:

(i) if the entity is an agency--the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(ii) if the entity is an organisation--the information is reasonably necessary for one or more of the entity's functions or activities; or

(b) subclause 3.4 applies in relation to the information.

3.4 This subclause applies in relation to sensitive information about an individual if:

(a) the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(b) a permitted general situation exists in relation to the collection of the information by the APP entity; or

(c) the APP entity is an organisation and a permitted health situation exists in relation to the collection of the information by the entity; or

(d) the APP entity is an enforcement body and the entity reasonably believes that:

(i) if the entity is the Immigration Department--the collection of the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the entity; or

(ii) otherwise--the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(e) the APP entity is a non-profit organisation and both of the following apply:

(i) the information relates to the activities of the organisation;

(ii) the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities.

Note: For permitted general situation , see section 16A. For permitted health situation , see section 16B.

Means of collection

3.5 An APP entity must collect personal information only by lawful and fair means.

3.6 An APP entity must collect personal information about an individual only from the individual unless:

(a) if the entity is an agency:

(i) the individual consents to the collection of the information from someone other than the individual; or

(ii) the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or

(b) it is unreasonable or impracticable to do so.

Solicited personal information

3.7 This principle applies to the collection of personal information that is solicited by an APP entity.

[132] APP5 provides that, at or before the time when an APP entity collects personal information, the entity must take reasonable steps to notify the individual of certain listed matters including:

> (a) The identity and contact details of the entity;
>
> (b) Where the entity has collected the personal information from someone other than the individual, or the individual may not be aware that the entity has collected the information, the fact that the entity has so collected and the circumstances of the collection;
>
> (c) The purposes for which the entity collects the personal information;
>
> (d) Consequences of non-collection;
>
> (e) Any other APP entity, body or person to which the entity usually discloses personal information of the kind collected by the entity; and
>
> (f) Information about what is contained in the entity's APP privacy policy.

Breaches of the Privacy Act

[133] Mr Lee asserts that Finlayson Timber has breached the APP's in several ways. Firstly, Finlayson Timber did not have an APP policy, let alone one that was freely and appropriately available. This is in breach of APP1.

[134] Secondly, it was Finlayson Timber which owned the scanners and software system for use with the scanners. Accordingly, Finlayson Timber received sensitive information (in the form of biometric templates and biometric information) about Superior Wood's employees when they registered for use of the biometric scanning system, and each time they used the system to clock on or off. Mr Lee submits that the receipt of such information is in breach of APP's 3 and 4.

[135] Mr Lee asserts that if he had complied with the Site Attendance Policy like all other employees, he would not have been giving his biometric template and information to only his employer; he would also have been allowing a separate corporate entity which was not his employer to receive that sensitive information, notwithstanding that it had never sought and never obtained Mr Lee's consent.

[136] Further, Mr Lee submits that Finlayson Timber also breached APP5 by failing to give the individuals whose sensitive information it received notification of that collection.

Employee record exemption

[137] It is acknowledged that within the Privacy Act there is an employee record exemption. It is as follows:

> **"7B Exempt acts and exempt practices of organisations**
>
> **…**

Employee records

(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.

[138] Employee record is a term defined in section 6 of the Privacy Act as follows:

"6 Interpretation

"employee record", in relation to an employee, means a record of personal information relating to the employment of the employee. Examples of personal information relating to the employment of the employee are health information about the employee and personal information about all or any of the following:

(a) the engagement, training, disciplining or resignation of the employee;

(b) the termination of the employment of the employee;

(c) the terms and conditions of employment of the employee;

(d) the employee's personal and emergency contact details;

(e) the employee's performance or conduct;

(f) the employee's hours of employment;

(g) the employee's salary or wages;

(h) the employee's membership of a professional or trade association;

(i) the employee's trade union membership;

(j) the employee's recreation, long service, sick, personal, maternity, paternity or other leave;

(k) the employee's taxation, banking or superannuation affairs.

[139] Mr Lee submits that if Superior Wood can rely on the employee records exemption to absolve itself of what would otherwise have been its clear breach of the Privacy Act forcing its employees to provide sensitive information in the form of biometric templates, Finlayson Timber cannot. Finlayson Timber did not employ Mr Lee or any other workers at Superior Wood. Accordingly, Mr Lee submits that each time Finlayson Timber received an

individual's biometric information, it was in breach of APP's 3, 4 and 5, which is made unlawful by s.15 of the Privacy Act.

[140] Mr Lee submitted that the exemption in section 7B of the Privacy Act can apply only to information held by an employee's employer. Mr Lee submitted that Superior Wood had informed its employees that the implementation of the scanners was necessary for the payroll management of 400 employees; far more employees than Superior Wood employed.

[141] Mr Lee submitted that it was reasonable to consider that another organisation within the Finlayson Group may have been collecting or using the information collected by the scanners to manage payroll across the Finlayson Group, or that Mitrefinch may have sought to use or collect the information.

[142] Mr Lee submitted in the alternative that if Superior Wood's collection of biometric information was found to be lawful on the basis that Mr Lee's biometric information is considered to be an 'employee record', then Superior Wood's direction to use the scanners was still unreasonable because Superior Wood failed to provide to Mr Lee sufficient information that would satisfy a reasonable person that Superior Wood was complying with its obligations under the Privacy Act.

[143] Mr Lee conceded that Superior Wood never in fact collected his sensitive information. However, Mr Lee submitted that Superior Wood's obligation to observe the APPs arose at the time that it took steps to collect Mr Lee's sensitive information and that Superior Wood breached the Privacy Act at that time.

Repeated breaches of the Privacy Act

[144] It is submitted that Finlayson Timber (as opposed to Superior Wood) was involved in a breach of the Privacy Act at least twice a day for around 150 Superior Wood employees, and accordingly had breached s.13 of the Privacy Act for repeated interferences with privacy. It was more serious, it is contended because the information is sensitive information, not just personal information. It is submitted that Superior Wood has also contravened s.13G of the Privacy Act by its involvement in the acts and practices which led to Finlayson Timber's unlawful receipt of sensitive information in breach of s.13G. It is said that it was Superior Wood's Site Attendance Policy and directions for compliance which were the means by which Finlayson Timber came to receive the sensitive information.

[145] Mr Lee submits that but for Superior Wood 'forcing' its employees to use the biometric scanners, the employees' sensitive information would not have been recorded on the scanners of the system behind them, all which belonged to Finlayson Timber, as opposed to Superior Wood.

Unlawfulness of the Site Attendance Policy and unfairness of the dismissal

[146] Mr Lee states that the Commission must determine if Superior Wood engaged in any act or practice that was contrary to, or inconsistent with one or more of the APP's. If so, Superior Wood will have acted contrary to its obligations under the Privacy Act unless an exemption applies under the Privacy Act.

[147] It is submitted that a person's dismissal will be harsh, unjust or unreasonable if, among other things, the dismissal has occurred in response to the employee refusing to obey an unlawful order. Further, it will be harsh, unjust or unreasonable if it is disproportionate to the gravity of the misconduct to which it purports to respond or has significant consequences for the employee's personal and economic situation.

[148] Mr Lee submitted that the direction to him, and to others, to use a biometric scanner in order to allow Superior Wood and possibly others to collect and use his biometric information was neither lawful or reasonable.

[149] It was submitted that if the direction was lawful and reasonable, Mr Lee's failure to obey it was not the kind of misconduct that would justify dismissal. There were reasonable alternatives available to Superior Wood other than dismissal, it was submitted.

[150] Mr Lee submitted that his consent to the collection of his sensitive information could only be given voluntarily. Mr Lee submitted that Superior Wood had sought to obtain Mr Lee's consent under duress, coercion or pressure by mandating the use of the scanners through the Site Attendance Policy which, as submitted by Mr Lee, had been introduced without consultation and further by 'stonewalling' Mr Lee's attempts to find alternatives to the use of the scanners and by threatening him with disciplinary action.

[151] Mr Lee submitted that Superior Wood acted recklessly or with contempt for the need to obtain Mr Lee's consent to the collection of his biometric information.

[152] Mr Lee submitted that Superior Wood never sought to obtain his express consent before attempting to handle his sensitive information, and failed to notify Mr Lee of matters which would have been reasonable in the circumstances, including the terms of Superior Wood's privacy policy and the corporate entity that would be collecting and using the information.

[153] It was submitted that Superior Wood was 'heavy handed' and 'capricious' in the way it attempted to force Mr Lee to allow unlawful collection/receipt of his sensitive information in circumstances where he had clearly expressed his non-consent. Mr Lee submits that Superior Wood took the view that his concerns about his privacy were irrelevant and it could force him to hand over sensitive information without giving him any assurances about the intended use or security of that information.

Was there a valid reason?

[154] Mr Lee submitted that Superior Wood's action were also inconsistent with APP 3.3 in that it was not reasonably necessary for Superior Wood to collect Mr Lee's sensitive information for Superior Wood's functions or activities. Mr Lee referred to the APP Guidelines which provide that 'reasonably necessary' collection of sensitive information does not refer to a use which is 'helpful, desirable or convenient', and will usually be 'reasonably necessary' if there are reasonable alternatives available.[19]

[155] Mr Lee submitted that the function or activity identified by Superior Wood as necessarily requiring the use of the scanners was timekeeping for payroll. Mr Lee submitted that while the scanners may be suitable and convenient for that activity, their use was not

reasonably necessary in place of other reasonable alternatives which Mr Lee had suggested, including the use of an employee number, password or timecard.

[156] Mr Lee submitted that he had proven himself to be a loyal and trustworthy employee. He had attempted to discuss his concerns about the scanners with Superior Wood and had sought to engage with Superior Wood about alternatives in good faith. Mr Lee submitted that the cost to Superior Wood in allowing Mr Lee some alternative means of identifying himself would not have been unreasonable.

[157] Mr Lee submitted that reinstatement to his previous position with Superior Wood is an appropriate remedy in the circumstances. Mr Lee also seeks compensation for his lost earnings resulting from his dismissal.

[158] In reply, to Superior Wood's submissions, Mr Lee submitted that it is irrelevant as to whether Superior Wood might have agreed to allow him to wear a surgical glove when using the scanner; there is no evidence that either party ever proposed the use of a surgical glove.

[159] Where Superior Wood asserts that its purpose in obtaining the biometric data of an employee is for a legitimate purpose, the obligation in the Privacy Act is more onerous than simply ensuring that the collection and use serves a legitimate purpose.

[160] It was submitted that where Superior Wood relies on the employee records exemption to avoid the conclusion that Superior Wood's conduct was unlawful under the Privacy Act and APP's, prior to the dismissal Superior Wood failed to provide Mr Lee with information that would satisfy a reasonable person that his sensitive information would not be collected or used by any third party, such that the exemption would apply.

[161] It is Mr Lee's contention that given the evidence of Superior Wood, it confirms, rather than dispels the impression that if he had used the biometric scanner, his sensitive information would be collected or used by third parties, including other parts of the Finlayson Group and MitreFinch.

[162] It is submitted that the collection of sensitive information is not 'reasonably necessary' on the basis that the alternatives are 'not satisfactory', or on the basis that the collection is considered reasonably necessary 'given the purpose for which the information would have been collected'. It is submitted that it is not sufficient to identify some legitimate general purpose behind the collection, such as health and safety or efficiency of the payroll function.

[163] Mr Lee suggests that it could not be said that the collection of biometric data was reasonably necessary in light of other reasonable alternatives such as a timecard or passcode. These other courses would not, Mr Lee contends, be expensive as Superior Wood had already decided to implement an expensive biometric identify verification system.

[164] As to whether the direction was unreasonable, Mr Lee contends that the question of reasonableness is directed not to the policy but to the direction given to the employee in the particular circumstances of the case. The direction that Mr Lee use the biometric scanner was not a direction that any reasonable employer in the position of Superior Wood would have given, in light of Mr Lee's objection and particular circumstances.

[165] Where the employer has stated that if it had respected Mr Lee's concerns, and agreed he need not comply with the policy, this would not 'have sent a good message', Mr Lee contends this is unsound. The characterisation of Mr Lee's objection as setting a precedent for employees to disobey directions 'as it suited them' ignored Mr Lee's good record of service to his employer and the nature of his objection.

[166] In an exchange with Mr Martin on Mr Lee's behalf, Mr Martin submitted that Mr Lee should be reinstated by the Commission. The following discussion was had:[20]

Commissioner: Well, it is not unlawful once they get their collection notice out, is it?

Mr Martin: That might be the case.

Commissioner: Then comes the consent issue.

Mr Martin: Yes, that might be the case, yes.

Commissioner: So you want him to be reinstated but he is free to not agree to use the scanner?

Mr Martin: Well, if the issue with the collection notices and the other issues haven't been dealt with, then the policy would still be unlawful and he wouldn't have to comply, but - - -

Commissioner: Let's say tomorrow the employer goes and issues collection notices and Mr Lee is reinstated. It is no longer unlawful, is it?

Mr Martin: That would seem to be the case.

Superior Wood's submissions

Valid reason for the dismissal s.387(1)(a)

[167] Superior Wood submitted that in considering if there was a valid reason for the dismissal, the Commission must determine whether, on the balance of probabilities, the conduct allegedly engaged in by the employee actually occurred.[21]

[168] It was submitted that a failure by an employee to follow the employer's lawful and reasonable directions can constitute a valid reason for dismissal.[22]

[169] It was submitted that a direction to comply with a policy must be in relation to a lawful policy which relates to the subject matter of employment or a matter affecting work and it must be reasonable. A policy will be reasonable if a reasonable employer, in the position of the actual employer acting reasonably, could have adopted the policy. A policy will not be unreasonable merely because a Commission member considers that a better or different policy may have been more appropriate,[23] and it is note the Commission's role to interfere with the right of an employer to manage his own business, unless he or she is seeking from the employee something which is unjust or unreasonable.[24]

[170] Superior Wood referred to the decision of Commissioner Holmes in *MEAA v Victorian Amateur Turf Club*.[25] Commissioner Holmes in that case considered that the use of a biometric hand scanner similar to the scanner in the present case was reasonable, and stated:[26]

> "*In relation to the privacy issue I am not satisfied that the system is any more intrusive than requiring an individual employee to enter their signature in a time book, user card clocking system or an electronically coded card".*

[171] It was submitted that there was a valid reason for the termination of Mr Lee's employment, namely that Mr Lee failed to comply with the Site Attendance Policy. Superior Wood submitted that the only significance of the scanner relying upon a biometric algorithm was that the biometric algorithm was the means by which the scanner was made completely secure and unable to be manipulated.

[172] It was submitted that there were no reasonable privacy concerns involved with the use of the scanners in addition to the collection of data relating to employee attendance at the workplace, which is a feature of all payroll systems regardless of their sophistication.

Notification of reason s.387(1)(b)

[173] It was submitted that Mr Lee was notified of the reason for the termination of his employment in the letter of termination.

Opportunity to respond s.387(1)(c)

[174] Superior Wood recognised that an employee must be given an opportunity to respond to the reason for termination before a decision to terminate is made.[27] Superior Wood submitted that the process of providing an opportunity does not require any formality and is to be applied in a common-sense way to ensure the employee has been treated fairly.[28] It was submitted that it is enough for an employee to be made aware of the precise nature of the employer's concern about the employee's conduct or performance and to be given an opportunity to respond to those concerns.[29]

[175] It was submitted that Mr Lee was provided with an opportunity to respond to the reasons for termination before the decision to terminate was made, through the meetings of 30 January and 6 February 2018.

Support person at discussions s.387(1)(d)

[176] It is not contested that Mr Lee was offered a support person at all relevant meetings.

Prior warnings s.387(1)(e)

[177] Superior Wood acknowledged that the Commission must take into account the period of time between an employee being warned about unsatisfactory performance and a subsequent dismissal.[30] The warnings given to an employee must identify the relevant aspect of the employee's performance which the employer is concerned with.[31]

[178] Mr Lee was issued with two warnings prior to the dismissal; during the meeting of 11 January 2018 and of 17 January 2018. Mr Lee was aware that Superior Wood was concerned about Mr Lee's conduct in refusing to use the scanners and to adhere to the Site Attendance Policy.

Size of the enterprise s.387(1)(f) and (g)

[179] It was submitted that this is not a relevant consideration.

Other considerations s.387(1)(h)

[180] It was submitted that sufficient information was provided by Superior Wood to Mr Lee to address his concerns about the nature of the information collected by the scanner. Mr Lee was informed that the scanner did not take a fingerprint. Superior Wood submitted that Mr Lee's objections to participating in its use are not sufficient to exempting him alone from the employer's objectives of preventing inaccuracy and fraud in its payroll, and improving safety.

[181] Superior Wood submitted that it had not breached the Privacy Act because the 'employee records' exemption under section 7B of the Privacy Act applies. The Explanatory Memorandum introducing the Privacy Act into Parliament stated the following:

> '….Acts and practices in relation to "employee records" are exempted as it is recognised that the handling of employee records is a matter better dealt with under workplace relations legislation.'[32]

[182] Relevant to the biometric data on the scanner at Superior Wood, it was submitted that the record is, in fact, held by the employer, Superior Wood. Simply because a copy is taken off-site, and stored on an associated entity's server in a fire-proof room does not mean that the employee record is not held by Superior Wood. It was submitted that any employer who put a copy of an employee record in a secure data storage facility off-site would lose the benefit of the employee record exemption which the legislation clearly intends that they have.

[183] It was submitted that even though the time and wages records generated as a result of the scanning is done by another entity, it is only the biometric data that is relevant for the purpose of this application, and it is exempt from the Privacy Act.

[184] Superior Wood submitted that any biometric information that would have been collected would have been reasonably necessary for Superior Wood's activities within the meaning of Schedule 3 of the Privacy Act and the National Privacy Principles given the purposes for which the information would have been collected; the improvement of the accuracy of Superior Wood's payroll function and the discharge of work, health and safety duties.

[185] I note that the National Privacy Principles referred to by Superior Wood were amended and replaced by the APPs by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*. However, Superior Wood's submissions on the improvements to its payroll and workplace health and safety functions remain relevant with respect to the APPs.

[186] Relevant to the failure by Superior Wood to provide to Mr Lee and other employees a collection notice, it is conceded this might be an issue for Superior Wood. However, it was submitted that because Mr Lee made it very clear that he would never agree to the provision of his biometric data, the time for collecting personal information about Mr Lee never arose. It was never going to arise because Mr Lee effectively said, "I was never going to agree, I told them that from day one, minute one, and I'm telling the Commission that today, I never did, I never have and I never will."[33]

[187] Superior Wood submitted that the dismissal was not harsh, unjust or unreasonable when regard was had to the fact that there was around 3.5 months of gentle persuasion.

Submissions on reinstatement

[188] It was submitted that the evidence of Superior Wood managers is they have lost trust and confidence in Mr Lee because of his refusal, alone amongst his peers, to comply with the Site Attendance Policy for no good reason. An employee who elects to be exempted from a policy directed towards honesty, accuracy and safety, which policy causes no harm to them, cannot expect to retain the requisite degree of confidence on the part of their employer.

[189] It was conceded that just because the person's role has been filled by another, on its own it is insufficient for a finding that reinstatement is not appropriate. It is just one factor to be taken into account in determining whether reinstatement is appropriate.[34] It was submitted that should the Commission find for Mr Lee, reinstatement would be inappropriate, and compensation should be awarded.

Submissions on compensation

[190] It was submitted that but for the termination, Mr Lee's employment would not have continued for much longer; only 2-4 weeks. This is so because, as stated by Mr Finlayson in his evidence, Mr Lee had demonstrated an unwillingness to follow the Site Attendance Policy which impacted upon Superior Wood's ability to manage Mr Lee's employment through Superior Wood's payroll system. Superior Wood submitted that Mr Lee's employment could not continue in the circumstances that he could not be paid under its payroll system.

[191] Mr Lee received two week's pay in lieu of notice when he was not entitled to any notice, as he employed as a casual employee.

[192] It was submitted that Mr Lee's efforts to mitigate his loss was not demonstrative in his initial evidence to the Commission. Further, if the Commission is inclined to award compensation to Mr Lee, it should be discounted to take into account his misconduct in not complying with the Site Attendance Policy.

Consideration

[193] I must now consider whether Mr Lee's dismissal was harsh, unjust or unreasonable. The criteria I must take into account when assessing whether the dismissal was harsh, unjust or unreasonable are set out in s.387 of the Act, extracted above at [8].

[194] In *Byrne v Australian Airlines Ltd*, McHugh and Gummow JJ explained the various permutations of 'harsh, unjust or unreasonable' which may result in a dismissal being considered 'unfair':[35]

> "…It may be that the termination is harsh but not unjust or unreasonable, unjust but not harsh or unreasonable, or unreasonable but not harsh or unjust. In many cases the concepts will overlap. Thus, the one termination of employment may be unjust because the employee was not guilty of the misconduct on which the employer acted, may be unreasonable because it was decided upon inferences which could not reasonably have been drawn from the material before the employer, and may be harsh in its

> consequences for the personal and economic situation of the employee or because it is disproportionate to the gravity of the misconduct in respect of which the employer acted."

[195] I am duty bound to consider each of the above criteria in deciding the outcome of this matter.[36] My considerations in respect of each the criteria appear separately below.

(a) Whether there was a valid reason for the dismissal related to the person's capacity or conduct (including its effect on the safety and welfare of other employees)

[196] Central to my consideration of this criterion is whether Superior Wood's action, in attempting to collect Mr Lee's biometric information through the use of the scanners was inconsistent with its obligations under the Privacy Act. Before doing so, however, I wish to determine whether, in my view, the introduction of the Site Attendance Policy was unjust or unreasonable.

[197] In the case of *Woolworths (t/as Safeway) v Brown (Woolworths*), a Full Bench of the Australian Industrial Relations Commission considered how and when an employer's policy will be reasonable to have been complied with, and stated:

> "What is reasonable will depend upon all the circumstances including the nature of the employment, the established usages affecting it, the common practices which exist and the general provisions of the instrument governing the relationship. A policy will be reasonable if a reasonable employer, in the position of actual employer and acting reasonably, could have adopted the policy. That is, a policy will only be unreasonable if no reasonable employer could have adopted it. A policy will not be unreasonable merely because a member of the Commission considers that a better or different policy may have been more appropriate. As the Full Bench observed in the *XPT Case*, albeit in a somewhat different context, it is not the role of the Commission "*...to interfere with the right of an employer to manage his own business unless he is seeking from the employees something which is unjust or unreasonable*." [footnotes omitted].[37]

[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.

[200] Relevant to the necessary consideration of the application of the Privacy Act, I consider that the information collected by the scanners meets the definition of 'sensitive information' under section 6 of the Privacy Act, as either biometric information that is to be uses for the purpose of automated biometric verification or biometric identification, or a biometric template.

[201] Superior Wood meets the definition of an 'organisation' and an 'APP entity' under the Privacy Act.[38] 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.[39]

[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.

[205] Rounding back to whether an individual consents to the collection of the information, it appears that the other employees of Superior Wood gave implied consent to the collection of their sensitive information by attending upon Mr Lithgow during November 2017 and registering their fingerprint algorithm to be used by the scanners. It is concerning that the employer, Superior Wood, did not provide to employees a collection notice stating what it would do with their information to ensure their sensitive information would be kept safe, and who, or which organisations the information might be shared with. Nor did Superior Wood or Finlayson Group have an appropriate Privacy Policy.

[206] The Privacy Act has been in force relevant to private enterprise since December 2001. It is concerning that a reasonably large employer did not have a suitable Privacy Policy in place in 2017.

[207] Further, on the information before the Commission, Mitrefinch did not have in place a Privacy Policy until May 2018, and Mr Douglass' evidence was poor and rather disturbing

relevant to the obligations on Mitrefinch to ensure it collects and uses personal and sensitive information in accordance with Australian privacy laws.

[208] Superior Wood first notified its employees about the implementation of the scanners and the collection of their sensitive information in the meeting of 25 October 2017, as described above at [19]. The employees of Superior Wood were merely informed that the scanners were being introduced and that they would be required to use them. Superior Wood did not inform its employees that the scanners collected the sensitive information of its employees, provide a 'collection notice' regarding the collection of their sensitive information or discuss the obligations imposed on Superior Wood in handling its employees' sensitive information.

[209] It is argued that because Mr Lee's biometric data was never collected, there was never a breach with respect to Mr Lee. In questioning from me to Mr Martin, he agreed that the breach was the failure by Superior Wood or by Finlayson Timber to provide to Mr Lee a collection notice.[40] The following exchange occurred:[41]

> Commissioner: Yes, but in Mr Lee's case, the sensitive information is never obtained.
>
> Mr Martin: No, but the policy that he refused to comply with was already unlawful because other people had had their sensitive information collected because of their compliance with the policy and hadn't received the collection notice.

[210] Mr Lee did not either expressly or impliedly consent to the collection of his sensitive information by the scanners. The Site Attendance Policy required Mr Lee to provide his sensitive information to Superior Wood for collection. By mandating Mr Lee to comply with the Site Attendance Policy, Superior Wood attempted to collect Mr Lee's sensitive information with his consent, however he continued to decline consent.

[211] As to whether Superior Wood or Finlayson Timber & Hardware Pty Ltd owned the scanners, on Mr Finlayson's evidence at the second hearing, I am satisfied that Superior Wood pays to the parent company an amount per month in the way of an administration fee for the use of the scanners. While there was no formal leasing arrangement to expressly state the use by Superior Wood, I accept that the scanner has been placed at the Superior Wood sites for the use of Superior Wood employees (and visiting employees and management), and the monthly sum of $1,250 is not insubstantial.

[212] Within APP6 the following is stated about related bodies corporate:

> 'Related bodies corporate
>
> 6.6 If:
>
> (a) an APP entity is a body corporate; and
>
> (b) the entity collects personal information from a related body corporate;
>
> this principle applies as if the entity's primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information.'

[213] In my view, having regard to [212] above, it matters little if the daily information of time and attendance, generated by the daily use of the scanners is gathered by Superior Wood or by the parent company owning the servers in place in a secure environment. Whether it is Superior Wood or the parent entity who is collecting the personal information, the APP6 applies.

[214] AUS IT Services Pty Ltd, looking after the data contained on the server knows its obligations relevant to the Privacy Act and has assured its client, Finlayson Timber & Hardware Pty Ltd that it will meet its Privacy Act obligations.

[215] At this point in time I am satisfied that the collection of the private and sensitive information was for a function or activity that was reasonably necessary. I am disturbed that none of the organisations, except the IT provider has in place a privacy policy, and I am concerned that there was a failure by Superior Wood to issue a collection notice.

[216] Relevant to APP3.5 which states that an APP entity must collect personal information only by lawful and fair means, having regard to some of the decisions issued by the Australian Information and Privacy Commission, this might include consideration of illegal telephone recordings and the like. Mr Lee's biometric data was not collected, as he did not provide his consent. The employer did not unlawfully press his hand into a scanner to provide a template. Mr Lee said he did not consent and therefore Superior Wood did not collect personal information.

[217] I must consider whether Superior Wood was exempt from acting in accordance with APP 3.3 by the operation of the s.7B(3) of the Privacy Act.

[218] During the hearing Mr Martin made the following statement:[42]

> "…….If Superior Wood was the owner of all the equipment and all the servers where it was stored, then they could potentially rely on the employee records exemption to say, "It's irrelevant, we're the only one collecting the information, so what we are doing is lawful." It is because in this case there was the collection by the other entity that isn't an employer that it affects the lawfulness and reasonableness of the policy.'

[219] The evidence of Mr Finlayson (as extracted at [75] - [103] above) was that the information collected by the scanners was not held by Superior Wood. The information was instead held by a third-party company, 'AUS IT', and the Finlayson Timber and Hardware Company. Mr Finlayson's evidence confirms that Superior Wood had not notified Mr Lee that the data collected by the scanners was held on servers owned by the Finlayson Timber and Hardware Company and maintained by 'AUS IT'.

[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.

[224] Mr Lee submitted that Superior Wood could not validly dismiss him for refusing to comply with the Site Attendance Policy as it could not lawfully direct him to consent to providing his sensitive information. Even if Superior Wood, or some other associated entity or every associated entity of Superior Wood provided to Mr Lee a privacy collection notice, informing him of each entity's obligations relevant to the Privacy Act, Mr Lee's evidence is that he would not, under any circumstances, provide his consent.

[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.

[229] Further, I note that the scanners allowed for additional safety benefits beyond simple attendance verification, such as reviewing site attendance on supervisors' phones. The other methods identified by Mr Lee do not provide such additional benefits.

[230] Overall, Superior Wood decided that the method of site attendance verification that would be implemented at its workplace was the biometric scanning system. It was within its rights as an employer to install the scanners and to create a policy governing the use of the scanners which its employees were mandated to follow in the course of their employment.

[231] Superior Wood made significant efforts to provide additional information about the scanners to Mr Lee and to allay his concerns about the collection of his biometric data. It appears from the evidence that Superior Wood may not have completely grasped the precise nature of Mr Lee's particular concerns regarding his biometric information, as opposed to his fingerprint. Nevertheless, Superior Wood gave Mr Lee repeated opportunities to explain his objection to using the scanners and made several attempts to indicate to Mr Lee that his continued employment with Superior Wood was dependent upon his adherence with the site Attendance Policy.

[232] It is clear that even if a privacy collection statement had been issued, it would not have allayed any of Mr Lee's concerns. Even at hearing, Mr Lee remains steadfast of the view that his fingerprint can be reconstructed from the biometric data obtained from the scanner. On the information available to the Commission, Mr Lee's concerns are incorrect. I understand his concerns and his distrust, and he is entitled to hold such views.

[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 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.

(b) whether the person was notified of that reason

[236] Mr Lee was repeatedly warned that his failure to use the biometric scanner after a reasonable trial period would result in his dismissal. I consider that Mr Lee was appropriately notified that the reason for his dismissal was his continued refusal to follow the Site Attendance Policy.

(c) whether the person was given an opportunity to respond to any reason related to the capacity or conduct of the person

[237] Superior Wood discussed with Mr Lee the importance of using the scanners throughout November and December 2017. After the commencement of the Site Attendance Policy, Superior Wood met with Mr Lee on six further occasions to discuss his continued refusal to adhere to the Site Attendance Policy. I consider that Mr Lee was given several opportunities to respond to Superior Wood's directions to use the scanners and to follow the Site Attendance Policy.

(d) any unreasonable refusal by the employer to allow the person to have a support person present to assist at any discussions relating to dismissal

[238] Mr Lee was offered the opportunity to have a support person present at meetings with the employer. At the meeting of 24 January 2018, Mr Gethin was in attendance as Mr Lee's witness and support person. At no time did Superior Wood refuse Mr Lee from having a support person present.

(e) if the dismissal related to unsatisfactory performance by the person—whether the person had been warned about that unsatisfactory performance before the dismissal

[239] Mr Lee was not dismissed for unsatisfactory performance. Mr Lee was dismissed on the grounds of conduct as a result of his refusal to abide by the Site Attendance Policy.

(f) the degree to which the size of the employer's enterprise would be likely to impact on the procedures followed in effecting the dismissal

[240] Superior Wood is a reasonably large employer, and within a larger parent company. I do not consider that the size of Superior Wood had any impact on the procedures followed in effecting the dismissal.

(g) the degree to which the absence of dedicated human resource management specialists or expertise in the enterprise would be likely to impact on the procedures followed in effecting the dismissal

[241] The employees of Superior Wood responsible for managing Mr Lee's concerns were not employed as dedicated human resource personnel. However, Superior Wood met and corresponded with Mr Lee on several occasions in attempting to understand his concerns about the scanners. Mr Lee was served with several verbal and written warnings about his refusal to use the scanners and abide the Site Attendance Policy. When Superior Wood formed the view that Mr Lee should be dismissed, it provided him with a letter of termination

[242] I consider that the involvement of dedicated human resource management specialists in the management of Mr Lee's concerns would have been unlikely to impact on the procedures followed in effecting Mr Lee's dismissal.

(h) any other matters that the FWC considers relevant

[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.

[246] I have had regard to a speech given by the then Deputy Privacy Commissioner, Mr Timothy Pilgrim to the Biometrics Institute on 27 May 2010. Whilst it might now be somewhat outdated, I consider for the benefit of those interested in biometric data collection, not necessarily related to employment-related matters, it is suitable to reproduce the entire speech:

> "**Privacy in Australia: Challenges and Opportunities**
>
> Speech by Timothy Pilgrim, Deputy Privacy Commissioner, to Biometrics Institute, 27 May 2010
>
> **Introduction**
>
> May I start by thanking the Biometrics Institute for this opportunity to speak, and for Leanne's warm introduction.
>
> Our Office welcomes the commitment the Biometrics Institute has just given to include representation from consumer organisations and academia on the next review panel for the Biometrics Institute Privacy Code. Our Office believes that independent reviews of industry codes are critical to their effectiveness.
>
> I am very pleased to be able to present to an audience of people so clearly at the forefront of biometric technology development and use. As you would all understand, research and planning is very important in achieving a project's objectives. So, today I will be talking to you about building privacy into projects early. If you are going to do privacy right, you need to think about privacy early and build it in from the start.
>
> Like so many emerging technologies, biometric technologies have the potential to improve our lives and offer great opportunities. Many of you will be motivated by the goal of providing society with modern, innovative solutions to tackle difficult-to-solve problems.
>
> But as you surge ahead along this path of innovation and problem-solving, other important aspects need to be considered as part of their development. And probably the most important of these, particularly in the field of biometrics, is privacy.
>
> Now I would like to be clear about something; technology is not the enemy of privacy. Technology can be privacy enhancing. Privacy can be an enabler, not a blocker for technology development. Our Office believes it is crucial that there is a conversation about privacy and its relationship with the evolution of biometric technologies.And this conversation needs to happen now more than ever, as these technologies continue to rapidly take hold in everyday transactions.
>
> It is **now** that we have the best opportunity to make sure that privacy is embedded in the design and operation of biometric technologies. Tacking privacy protections on at the end is never the best outcome. Last minute considerations can be costly and

complicated for agencies and organisations, and potentially less effective in protecting individuals.

Today, I will emphasise two key messages. The first is that, for biometric technologies to be successful, individuals need to be able to trust that their privacy is not being eroded and, if possible, being enhanced. Without that crucial ingredient of trust, the industry in which you are all involved will struggle to thrive. Without the buy-in of the society in which you are operating, biometric technologies will not be able to produce the genuine solutions they aim to provide.

And the second message is that, for biometric technologies to flourish in a way that genuinely meets the community's needs and expectations, they need a nationally consistent regulatory environment. I will speak more about this later.

But first, I'd like to talk a bit more about the role privacy should play in the development and use of biometric technologies.

Biometric information and privacy

The way that governments and organisations handle biometric information is something that many people, quite understandably, feel very strongly about. This is because biometric information is about a person's physical characteristics. When we collect biometric information from a person, we are not just collecting information **about** that person, but information **of** that person.
Biometric information cuts across both information privacy and physical privacy. It can reveal sensitive information about us, including information about our health, genetic background and age, and most importantly, it is **intrinsic** to each of us.

The very nature of biometric information is one of its major advantages in terms of its powers of identification. However, this same attribute can also create significant privacy risks.

This is why developers and users of biometric technologies always need to have one eye on the solution the technology is being developed and used for, and the other eye on privacy outcomes. If you don't watch both, you will not be able to achieve either.

It might be a good time to talk briefly about how privacy is regulated in Australia.

The Privacy Act

I know that many of you will have a good knowledge of privacy laws. However, I still think it's useful to provide just a quick Privacy 101 update - some of the most important things you need to know about the current privacy regulatory framework and the role of our Office.

The first thing to note is that the Privacy Act is mainly about information or data protection - not about bodily or territorial privacy.

The Privacy Act protects 'personal information', which means:

> information or an opinion [...], whether true or not, and whether recorded in material form or not, about an individual whose identity is apparent, or can be reasonably ascertained, from the information or opinion.

The way organisations and agencies handle biometric data is only regulated by the Privacy Act to the extent that the data is also 'personal information'.

Second, it is important to realise that privacy, under the Privacy Act, is not an absolute right. The Privacy Act recognises that privacy needs to be balanced against other competing interests, including the desirability of the free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way. The Act is about balancing a range of interests, and that is the way our Office approaches its responsibilities.

Technology development

While the Privacy Act was designed to be technologically neutral, and while our Office believes that it has been effective in regulating flows of personal information since it was introduced in 1988, a great deal has changed in the way society conducts itself since then. Rapid advances in technology over the decades have presented significant challenges for regulation of personal information-handling in Australia.

Developments in biometric technologies have been at the forefront of this change. Back when the Privacy Act was introduced in 1988, many biometric technologies were largely confined to science fiction movies. Of course, a few, such as the use of fingerprints in law enforcement, were well established. However, the concept that biometric technologies could become part of our everyday consumer transactions was almost unthinkable.

A person standing in line at a bank branch in 1988 would struggle to conceive a future where they could phone their bank, be identified by voice recognition technology, and transact from the comfort of their own home. Yet today, this is a reality.

A worker signing a time sheet as they arrived at work in 1988, would struggle to conceive a time when they would be required to have a fingerprint scanned to clock on. Yet for some people today, this is a reality.

A young adult entering a nightclub in 1988 would struggle to conceive a future where they would have to submit to a face scan before being allowed entry. This would have been the crazy plot of some futuristic television show. But today, this is also a reality.

We are likely to continue to see increasing use of biometric technologies like those I have just mentioned, as well as iris scanning, palm scanning, and many others, in ways that we cannot predict. Assuming that these new technologies are developed in a way that is genuinely sensitive to privacy, this need not necessarily be a bad thing.

Biometrics - neither good nor bad

What is interesting about biometric technology is that we tend to hear both that it is good and bad for people's privacy.

On one hand, we hear that biometric technologies enhance privacy. For example, voice recognition technology is being rolled out in some call centres to identify callers, leading to more effective protection of clients' personal information.

On the other hand, we hear that biometric technology has the potential to invade our privacy. For example, in the film *Minority Report*, individuals confront ubiquitous iris scanning infrastructure and technology which allows their every activity to be tracked.

How do such obviously divergent views on privacy and biometrics coexist?

The answer is: because biometric technology is what we make it. Biometric technologies are not inherently good or bad for privacy, and privacy is not a blocker to the use of biometric technologies. These technologies can become good or bad for privacy depending on how they are designed, developed and deployed.

This is one of the key messages that I would like to communicate to you today. By considering projects involving biometric technologies in the context of privacy, and by building in privacy from the very beginning of the design phase, we can ensure that biometric technologies do not impinge on, but actually enhance, the privacy of individuals.

Enjoying the benefits of biometric technologies does not also mean we have to give up other freedoms or rights. Biometric technology has a lot to offer. Let's take responsibility to develop biometric systems carefully so that they achieve their aims while protecting privacy.

How to build privacy in

Our Office encourages all agencies and organisations to conduct Privacy Impact Assessments when commencing projects that are likely to impact on privacy to **design it in**. Earlier this month, in Privacy Awareness Week, we launched a new version of our Privacy Impact Assessment Guide, catering for both organisations and agencies.

Building privacy in from the start is cheaper and more effective than considering it only as an afterthought. Most importantly, projects and products that have been through a comprehensive privacy planning process are likely to inspire the trust of the community, have greater take-up and success, and so build your organisation's reputation.

The essential ingredient - trust

I have already mentioned trust a few times. Trust is a major factor in consumers' decision-making processes. In fact, in the Community Attitudes to Privacy research commissioned by our Office in 2007, 36 per cent of people stated that they had decided not to deal with an organisation because of concerns about how their personal information would be handled. This shows that individuals' perceptions about personal information can often dictate their consumer decisions.

It may, or may not, surprise you to hear that government departments actually enjoy a high level of trust from the community. In fact, that trust has been growing.73% of people surveyed said they believed that government departments were trustworthy

when it came to how they collected and used personal information. This is in comparison to 64% in 2004 and 58% in 2001.

The numbers for private sector organisations were generally lower that this, with 58% of people considering 'financial organisations' to be trustworthy, 37% for retailers and 17% for businesses selling goods over the internet.

No agency or organisation can ever afford to be complacent about trust. They can lose this trust and their reputation overnight if they sustain a major breach of personal information or handle personal information poorly.

And as I mentioned, many consumers will vote with their feet if they suspect an organisation may mishandle their personal information. This statement is particularly relevant for audience members here today, given that many consumers feel that biometric data is even more sensitive than other forms of personal information.

I should also note here that we are currently conducting several investigations including an own motion investigation into the scanning of driver's licences and the separate collection of biometrics like finger prints at night clubs and other entertainment venues. This includes looking at the technology and the processes involved. As these are ongoing investigations I cannot discuss any details but it does illustrate the importance of getting the technology and the business practices right from the start.

I note with interest that the Biometrics Institute is aware of the importance of community trust and confidence in an organisation's information-handling practices. The preamble to the Biometrics Institute Privacy Code states: *"only by adopting and promoting ethical practices, openness and transparency can these technologies gain widespread acceptance"*.

For agencies, it is even more vital to be careful to incorporate privacy principles into their operations as, in many cases, individuals may not have a choice about whether or not they participate in that agency's systems or operations. A poorly designed project incorporating biometric technology can cause considerable embarrassment or worse for government and serious repercussions for individuals.

Working with new technology is challenging, but it can also be very rewarding. If you're pioneering or implementing new biometric technologies, or any new product or service that impacts upon personal information, our Office encourages you to rigorously consider any privacy implications that may arise. By doing this, you place yourself ahead of the game, and are more likely to inspire the trust and confidence of your consumers and the community.

National consistency

There's another issue that I would like to discuss with you today. It is a little more technical, but is no less significant. It relates to the array of laws and regimes that govern the handling of personal information, including biometric information, in Australia.

As most of you will be aware, the Privacy Act is 'principles based'. There are 11 Information Privacy Principles (IPPs) for Australian Government agencies, and 10 National Privacy Principles (NPPs) for business. These principles govern how those agencies and businesses handle personal information, including its collection, use and disclosure, security and destruction.

However, the Privacy Act has some exceptions. For example, it does not cover most small businesses. Nor does it cover state government agencies. To bridge this gap, some Australian states have introduced their own laws covering their public sector.

Navigating the complex relationship between state and national laws is a familiar story in our federation, but this is little consolation for organisations and agencies trying to understand their privacy obligations.

In our current regulatory environment, some users of biometric information may fall outside of our Office's jurisdiction, and may not be required to comply with the Privacy Act.

Private sector organisations bound by the NPPs that perform some functions under contract to a state or territory government may have to comply with different laws for that work. As well, organisations contracted to Australian Government agencies may have to comply with the IPPs for functions performed under the contract, and the NPPs for their other functions. Confused? Well, it's not surprising.

And what is the main implication for biometrics? With different laws applying to different kinds of organisations and agencies, we risk having different standards applied to organisations and agencies conducting similar activities.

Information flows do not stop at state borders. Many large organisations have a presence in some or all Australian states and territories. In our modern, integrated economy, it makes little sense and can be very expensive to require organisations to handle information differently in different states and territories, even if these differences are often only minor.

As I'm sure you can see, the system that is currently in place can be quite complex. This is a challenge indeed. However, I'm glad to be able to inform you that there are genuine opportunities for improvements on the horizon.

Changes in the pipeline

As many of you will be aware, the Government has announced its intention to make major changes to privacy law in Australia. The Australian Law Reform Commission (ALRC) delivered a report to the Government in May 2008 recommending 295 changes to Australia's privacy framework. The Government outlined its first stage response to the Report in October last year, putting forward its position on 197 of the ALRC's recommendations.

The Government has said that it intends to release exposure draft legislation reflecting these changes during 2010.

A number of the recommendations that the Government has decided to adopt will have significant, and hopefully positive, impacts for the environment in which biometric technologies must operate in Australia. I'd like to explain some of these to you now.

Single set of privacy principles

As I mentioned earlier, in the Privacy Act, there are two sets of privacy principles.

In what is probably the key reform proposal of all of the ALRC's 295 recommendations, the Government announced that it sees the wisdom in replacing these two sets of principles with a single set of principles to cover all entities that are now covered by the NPPs or the IPPs.This means that, for the first time, Australian Government agencies will have the same obligations as private sector organisations covered by the Act (of course with a few exceptions).

So what does this mean for users of biometric data? This represents a significant step towards national consistency in the regulation of privacy and biometrics. For the first time, one set of rules will cover the biometrics field at a national level.

Biometric information as sensitive information

As I mentioned earlier, when we collect biometric information from a person, we are not just collecting information **about** that person, but information **of** that person. Recognising this fact, the Government has accepted the ALRC's recommendation that biometric information be treated as 'sensitive information' under the Privacy Act.

As it stands, the Privacy Act regulates the handling of personal information generally. The NPPs also contain extra protections specifically dealing with what is termed 'sensitive information', whereas the IPPs do not. The new, unified set of privacy principles will apply the higher protections applying to sensitive information to both agencies and organisations.

Sensitive information is a subset of personal information and includes information about things such as:

- racial or ethnic origin
- religious beliefs or affiliations
- criminal record information
- health information.

The ALRC neatly explains the rationale behind treating biometric information as 'sensitive information':

'Biometric information shares many of the attributes of information currently defined as sensitive in the Privacy Act.It is very personal because it is information about an individual's physical self. Biometric information can reveal other sensitive information, such as health or genetic information and racial or ethnic origin. Biometric information can provide the basis for unjustified discrimination.'

What this change will mean then is that organisations and agencies will only be able to collect sensitive biometric information about an individual in defined circumstances, including where:

- the individual has consented to the collection
- the collection is authorised or required by or under law, or
- the collection is necessary to prevent a serious threat to the life, health or safety of any individual.

This change will give individuals greater confidence that their sensitive biometric information will be appropriately treated by both agencies and organisations. And as you know, confidence is an important ingredient in building up trust.

This change will also ensure that both agencies and organisations have consistent obligations regarding the way they handle biometric information.

Technological neutrality

Importantly, the Government has also committed to ensuring that the Privacy Act remains technologically neutral. What this means is that the Act will continue to regulate information handling without referring to specific technologies.

This is important because it gives the Privacy Act the flexibility to be relevant to new technological realities as they present themselves.

The current Privacy Act was introduced in 1988 - a time when many people were only just buying their first microwave. People did not have access to the internet, mobile phones and an array of other technologies, including biometric technologies, that are central parts of our lives today. The principles that underpin the Privacy Act are even older, having originated in the 1980 OECD Privacy Guidelines.

It is a testament to the success of the principle of technological neutrality that the Privacy Act has been able to regulate personal information flows in Australia for more than 20 years without major difficulties.

Of course, technological neutrality does not mean that we bury our heads in the sand when it comes to technological change. Our Office believes that we can have technological neutrality of privacy laws while still having laws that are technologically relevant. We believe that technological neutrality allows the Privacy Act to be adequately flexible to accommodate technological change. What we don't want is a privacy regime that goes out of date every time technology changes!

Privacy codes

Going hand-in-hand with the concept of technological neutrality is the proposal to expand the Privacy Commissioner's powers in relation to privacy codes.

At present, industry groups are able to propose the introduction of a privacy code in a specific area. If the code has protections equal to or stronger than the NPPs, the Privacy Commissioner can approve it, and any organisation that opts in to the Code

must comply with it. Our Office can handle complaints about breaches of privacy codes.

Many of you here today will of course be familiar with one such code - the Biometrics Institute Privacy Code although our Office notes, regrettably, the low take up of the Code by businesses who are members of the Institute. We would encourage you to look again at the benefit in signing up to the higher privacy protections afforded to individuals by the Code, such as demonstrating to your clients your commitment to good privacy practice.

As well our Office welcomes the Institute's recent development of the Privacy Awareness Checklist which each member has been asked to complete when renewing their membership.

Under the proposed changes to the Privacy Act, the Privacy Commissioner will be able to request that an organisation or industry body develop a Privacy Code binding specified organisations. If an appropriate code is not developed, the Commissioner will be able to develop and impose one.

Of course, our preferred approach is to allow industries to take responsibility for their privacy obligations, and we are confident that this will happen. The Office encourages your industry to be proactive in its approach to privacy, and as I mentioned before, to **build privacy into projects**, rather than simply bolting it on.

However, this code-making power will allow our Office and industry the flexibility to ensure that certain fields dealing with specialised kinds of information and technology can be regulated appropriately, and in more detail than in the Act if necessary. This will give the Office the power to respond in a timely manner to new technologies with specific privacy issues, without needing a Privacy Act legislative change, which can be a very time-consuming and uncertain process!

Consistent laws in states and territories

With all of these changes planned in the sphere of privacy law, particularly with the use of biometric technologies, you could be forgiven for feeling slightly intimidated. My advice to you is not to be overwhelmed by the challenges that come with change, because the developments unfolding before us actually present great opportunities:

- the opportunity to develop consistent privacy laws across the public and private sectors in Australia
- the opportunity for all of us in the room to get ahead of the game, and start planning for the future
- and, perhaps most significantly, the opportunity for parliaments across Australia to take the new national laws as a model, to simplify and make consistent information-handling laws across all jurisdictions.

I refer again to the example I used earlier of some organisations needing to be conscious of both the NPPs and the IPPs and possibly even state privacy legislation. Our Office can see a future where laws across the country relating to information handling, including the regulation of biometric technologies, will be aligned. With a

simplified national privacy regime, government and organisations would at the same time have a reduced compliance burden and greater certainty of their obligations.

Conclusion

So in concluding let me say again that there is nothing wrong with acknowledging that biometric technologies have the potential to offer our society many great benefits.

Equally though, done badly, the development and use of biometric technologies has the potential to impinge on individual privacy and thereby risk undermining community confidence in such technologies. Once that community confidence evaporates, so too does much of the potential that might have made the technologies attractive in the first place. This is why it is important to address and build in privacy now.

If, as I suspect it is, the ultimate goal of the work of this audience is to devise, build and use innovative technological solutions the work you do is too important to risk jeopardising good results with poor privacy protections.

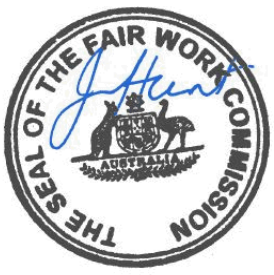
It is also vital that the environment in which these biometric technologies are developing be simple and nationally consistent to allow them to flourish in a considered, rather than an ad hoc, fashion. By having a simple, clear, nationally consistent environment, everybody knows where they stand, and individuals can be more confident that agencies and organisations will appropriately safeguard their privacy. In a word, it will generate **trust**.

Thank you."

Conclusion

[247] Having considered each of the matters specified in s.387, including whether there are any other relevant matters which make Mr Lee's dismissal harsh, unjust or unreasonable, I am satisfied that the dismissal of Mr Lee was not in all the circumstances harsh, unjust or unreasonable. Accordingly, I find that Mr Lee's dismissal was not unfair.

[248] The application is dismissed.



COMMISSIONER

Appearances:

Mr C. Martin of Counsel for the Applicant

Mr A. Herbert of Counsel for the Respondent

Hearing details:

15 June 2018.
Brisbane

10 August 2018.
Brisbane

Final written submissions:

Closing submissions for the Applicant, 2 July 2018.
Closing submissions for the Respondent, 25 June 2018.

Printed by authority of the Commonwealth Government Printer

<PR609918>

---

[1] Exhibit R2, Statement of Mr Ian Swinbourne, Annexure PS5.

[2] s.384(2) *Fair Work Act (2009)*

[3] PN104.

[4] PN117.

[5] PN121.

[6] PN135 – PN138, PN141, PN142.

[7] PN157 – PN167.

[8] PN177.

[9] PN178.

[10] PN183.

[11] PN205.

[12] PN215.

[13] PN217 – PN220.

[14] PN354.

[15] PN364.

[16] PN269.

[17] *Austal Ships Pty Ltd v Schrier* (AIRCFB, Ross VP Drake DP, Dight C, 13 August 1997).

[18] *Australian Telecommunications Commission v Hart* (1982) 43 ALR 165, 170; *Bayley v Osborne* (1984) 10 IR 5, 8; *Izdes v LG Bennet & Co Pty Ltd* (1995) 61 IR 439, 449.

[19] Australian Privacy Principle Guidelines, B.113 – B.115.

[20] PN828 – PN835.

[21] *Edwards v Giudice* (1999) 94 FCR 561.

[22] *Lambeth v University of Western Sydney* [2009] AIRC 47.

[23] *Woolworths (t/as Safeway) v Brown* [2005] AIRC 830.

[24] *Enginemen v State Rail Authority (NSW)* (1984) 295 CAR 188.

[25] Print P4608 [AG802039].

[26] Ibid, [50].

[27] *Crozier v Palazzo Corporation Pty Ltd* (2000) 98 IR 137.

[28] *RMIT v Asher* [2010] 194 IR 1.

[29] Ibid, 14 – 15.

[30] *Johnston v Woodpile Investments trading as Hogs Breath Café – Mindarie* [2012] FWA 2.

[31] *Fastidia Pty Ltd v Goodwin* (AIRCFB) Print S9280.

[32] *Privacy Amendment (Private Sector) Bill 2000*, Explanatory Memorandum (House of Representatives)

[33] PN924.

[34] *Smith v Moore Paragon Australia Ltd* (2004) 130 IR 446. [15].

[35] (1995) 185 CLR 410, 465.

[36] *Sayer v Melsteel* [2011] FWAFB 7498, [20].

[37] *Woolworths (t/as Safeway) v Brown* [2005] AIRC 830. [35].

[38] *Privacy Act 1988* (Cth) s.6, "APP Entity"; s.6C.

[39] Ibid, Schedule 1, APP 3.3.

[40] PN777.

[41] PN780 – PN781.

[42] PN816.