FWC gives the finger to employer use of biometric tech

Fingerprint, eye scanners, face and voice authentication; technology that was once confined to science fiction is increasingly common, including in the workplace. However, the Fair Work Commission has put up a cautionary hand, finding that an employer's use of mandatory fingerprint technology breached the Privacy Act.

Background

The employer, Superior Wood, rolled out biometric fingerprint scanning to track employee attendance. Its reasons were genuine. The new system was way more efficient than the old paper based sign-in/out process.

The roll out was going great until one of Superior Wood's 150 employees refused to hand over his fingerprint out of concern for the company's use and protection of his biometric info. After a long but unsuccessful process of trying to convince the employee he had nothing to worry about, Superior Wood dismissed him for failing to follow a lawful and reasonable direction.

Outcome

The case focused on whether mandatory participation in fingerprint scanning was reasonable.

On appeal, the FWC's Full Bench determined that it was not, because the mandatory system fell foul of the Privacy Act. Superior Wood:

- did not have a clear privacy policy about its management of the biometric data;
- did not have the employee's consent to collect his biometric data, which is "sensitive information" under the Privacy Act; and
- did not notify employees of required matters under the Privacy Act.

Wesley Rogers
Workplace Relations Counsel

+612 8216 3035
Email Wesley

Justin Cudmore
Partner

+612 8216 3015
Email Justin

Marque Lawyers Pty Ltd
Level 4, 343 George St
Sydney NSW 2000

Superior Wood sought to rely on the exception under the Privacy Act for "employee records". However, by drawing what we consider to be an artificial line, the Full Bench said the exception only applied once Superior Wood actually collected the employee information. In other words, collection of the biometric data was governed by the Privacy Act, but its use once collected was not (because the employee records exception then applied to it).

Implication

We certainly don't advocate for a world in which employers can literally collect employees' blood, sweat, and tears without following some form of due process. However, unless appealed (likely), the Full Bench's decision is problematic. Employers have long been in the habit of collecting employees' personal and sensitive information on the basis that the Privacy Act doesn't apply at all.

For example, employers direct employees to undertake criminal background checks, attend fitness for work assessments, or undertake drug and alcohol testing. This can lead to the collection of personal and sensitive information. This decision draws into question the lawfulness and reasonableness of such directions, particularly if the employee refuses.

In the circumstances, employers would be wise to revisit their privacy policy to ensure it captures personal and sensitive information collected from employees. While we expect a further appeal to the Federal Court, regardless of the outcome of the case, with the increasing prevalence of biometric scans and similar technology, it's good practice to give employees fair notice and relevant info before you seek to snatch up their fingerprints.

Questions? Give us a call.

Ph : +61 2 8216 3000
Fax: +61 2 8216 3001

Visit Website