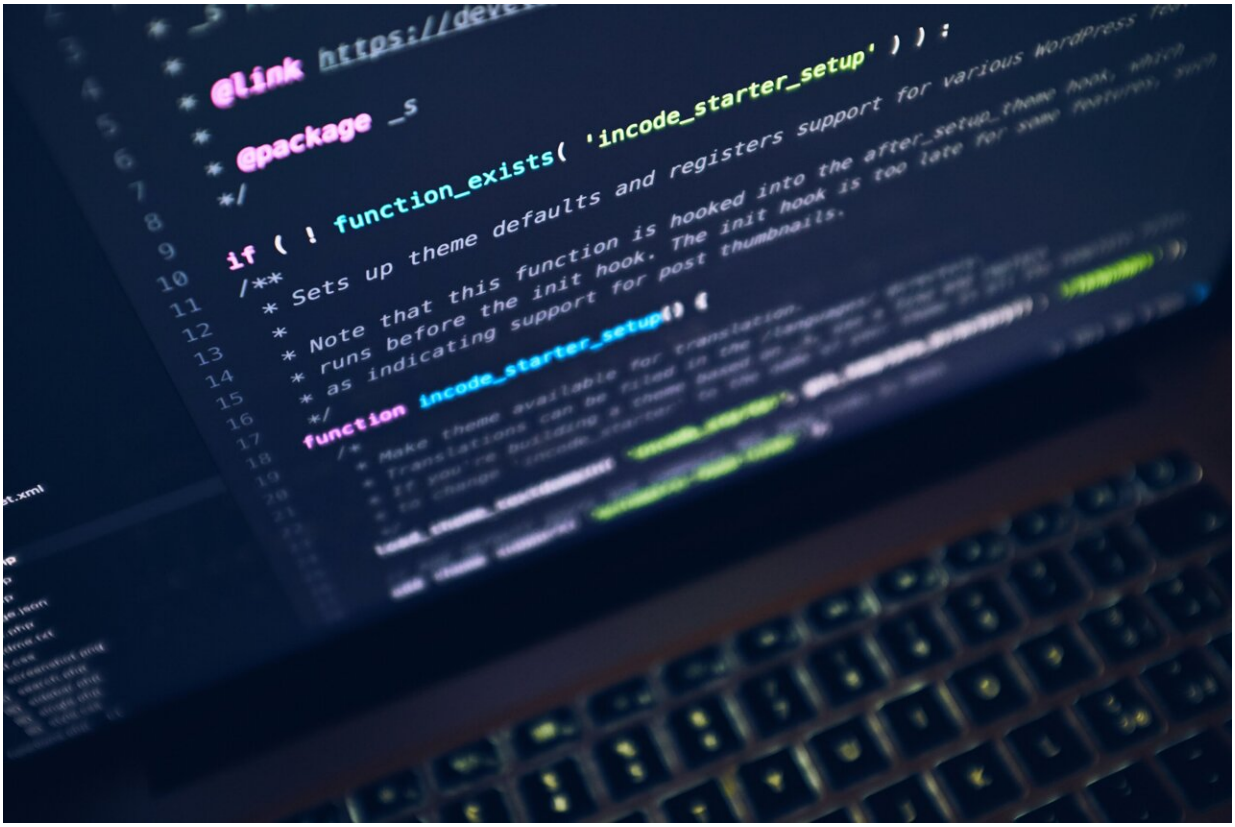
Biometric recognition technology in the workplace

June 3 2019, by Peter Holland, Tse Leng Tham



Credit: Unsplash/CC0 Public Domain

In *Back to the Future II* (1989), fingerprints are used to lock and unlock doors. It's a benign technology, apart from the rise of "thumb bandits" who amputate thumbs. *Gattaca* (1997) envisages a bleaker future, where

corporations collect DNA samples and genetic discrimination reigns.

Three decades on, "biometric recognition" technology is no longer science fiction. Should we embrace it or fear it?

That question faced Jeremy Lee, a sawmill worker in the town of Imbil, Queensland. when his employer, Superior Wood Ltd, introduced fingerprint scanning to verify clock-on and clock-off times.

Lee refused to comply. He was sacked as a result.

Lee then lodged an unfair dismissal claim in the Fair Work Commission. His claim was rejected last November.

But last month, Lee won his case on appeal before a full bench of commissioners.

Their ruling was particularly critical of the employer's lack of process and failure to understand its employees' right to privacy.

It's concerning management appeared to not understand the sensitivity of such data, and believed it had the right to demand it for something so mundane.

But what is most disturbing about this case, the first of its kind in Australia, is that just one employee out of about 400 resisted having their biodata taken. Every other employee acquiesced, despite management failing to provide any information about how it planned to store and protect such sensitive data.

Boundaries of consent

Biometrics refers to any technology that measures and analyses unique

physical and distinctive behavioral characteristics considered innate, immutable and unique to the individual.

Physiological markers include fingerprints, hand geometry, eyes and facial features. Behavioural markers include gait or voice patterns.

You don't have to look far to see these technologies in use. Fingerprint and facial scanning is now common as a security measure on phones and computers.

The advantages are obvious. The drawbacks less so.

The problem is when they are used by others to collect information about us.

In Australia, our political system may protect us from the prospect of biometric surveillance becoming omnipresent, as in the case of China, but we do face the potentially coercive power of employers wanting to use it.

Their reasons may be benign, possibly even quite compelling, but demanding that information might still cross a line that infringes privacy rights.

Once we agree to give up those rights, what guarantees do we have the information won't end up being used for other ends, legal or illegal?

Biodata is forever

This is why you, like Jeremy Lee, should be concerned.

Biometrics information can reveal a huge amount of information about you. If may even reveal information you don't know. Fingerprint data,

for instance, could potentially detect genetic disorders.

There needs to be clear boundaries, so information can only used for the purpose to which an employee has actively consented. Otherwise there is potential for systematic discrimination in recruitment, promotions and conditions of employment.

Perhaps an even greater risk is the security of this data.

Biometric data is vulnerable as any other digital form in an era of sophisticated hacking. It could prove just as valuable to criminals as credit-card details.

Cards can be replaced and passwords changed. Biodata cannot. The level of security protecting biodata should be much greater.

In the case of Jeremy Lee vs Superior Wood, the company admitted the data was stored at multiple sites with access by multiple sources.

Lee ultimately won his case because the commissioners decided the company had not abided by the Privacy Act (1988). That law says collecting sensitive information should be "reasonably necessary" – in this case there were other ways to verify when employees clocked on and off. It also prohibits collecting sensitive information without an individual's consent.

Thanks to Jeremy Lee, we now know any employer seeking to collect biometric data has the same obligations. And any employee has the right to object.

Provided by The Conversation