

# The Advocate

A regular newsletter for clients of MGZ Employment Law



## Use of Facial Recognition Technology in Business

The Privacy Commissioner recently released its determination on the trial of Facial Recognition Technology (“FRT”) across some of the Foodstuffs North Island (“FSNI”) stores.

The key concerns for the Privacy Commissioner in its inquiry were the justification for implementing FRT, and the way in which the technology would operate in practice.

### *Issue One: Justification*

For use of FRT to be justified, the information must be collected for a lawful purpose and collection of the information must be *necessary* for that purpose.

The Privacy Commissioner determined that FSNI had a lawful purpose for using FRT. Being “*to reduce the incidence of serious behaviours affecting its staff and customers*” and “*to reduce the incidence of high value theft, burglary and robbery by repeat offenders, to reduce the most serious financial losses*”.

### *Issue Two: Necessity*

When considering whether collection was necessary, the Privacy Commissioner considered whether FRT was actually effective in meeting the purpose that it was rolled out for. The Privacy Commissioner found that the trial showed FRT was an effective way to achieve its purposes, and that there was a substantial difference in reducing rates of serious recidivist crime in stores. Other

less intrusive measures were not sufficient on their own to address the issues the stores were facing.

*How the FRT model operated through a “privacy lens”*

The Privacy Commissioner noted that “[t]he success or failure of FRT depends on how each step of the whole operating model works. Applying a privacy lens to each of those steps enables a business to identify and eliminate or reduce potential problems that could harm people, undermine the purpose of using FRT, or damage public confidence in the business.”

The operating model needed to either remove privacy risks or, if the risk could not be removed, it needed to be reduced to an acceptable level. In its determination, the Privacy Commissioner noted the privacy safeguards employed throughout the system were sufficient to reduce the actual degree of intrusion that the FRT imposed on individuals.

The key safeguard that was implemented was the automatic and immediate deletion of non-matched images. This limited the information being stored to only that which was necessary. A watchlist was set up to identify “*matches*”. Alerts for matches could initially be made through the software, but would require a second check by a human.

FSNI also implemented information security controls, it limited the number of staff with access to the information to a small number of key staff, and training was provided to those staff.

Further, a process was set up for and information provided to customers about the operation of FRT and how they could access or correct their personal information held by the store. The operating model would also be subject to review and monitoring.

In summary, and noting the significant and widespread privacy implications of such technology being implemented, the Privacy Commissioner ultimately found that it complied with the Privacy Act 2020.

Although the trial is considered a success for FSNI, the Privacy Commissioner emphasised it was not a green light for all businesses. The trial and process by which the FRT was implemented highlights the need for justification of utilising FRT for each individual business. Further, having clear communication with people affected, and having policies and practices covering the implementation of the technology, as well as the use, access and storage of the information it collects will be essential. Technology is ever-evolving in the employment context, and this is a new development. If your business is considering implementing technology such as FRT, please reach out to us for assistance.



## ER Seminars - 2025

Our first two seminars of the year sold out. Don't miss out on the final one for 2025 being held on:

**Tuesday 14 & Wednesday 15 October 2025**

Further information on the course can be found on our website – [www.mgz.co.nz/training](http://www.mgz.co.nz/training) If you wish to enrol email your contact details to [carey@mgz.co.nz](mailto:carey@mgz.co.nz)

## Theft by Employer – New Crimes Act Offence

An amendment to the Crimes Act 1961 has been enacted that provides it is now a criminal offence for an employer to intentionally fail to pay money owed to an employee either under an employment agreement or employment legislation. However, an employer will have a defence where they can show that they had *reasonable excuse* for not paying the money owed to the employee.

This means that separate proceedings to that brought in the employment jurisdiction could be brought and prosecuted in the criminal jurisdiction.

Key distinctions between this new offence and proceedings brought for recovery for wages/other money owed in the employment jurisdiction include that the criminal jurisdiction is subject to a higher standard of proof. The prosecution would have to prove *beyond reasonable doubt* that the employer *intentionally* and *without reasonable excuse* failed to pay money owed to an employee. Whereas in the civil jurisdiction, the plaintiff bears the burden of proving to the balance of probabilities, meaning “*more likely than no*”.

An employer who is convicted of theft under this provision is liable to a term of imprisonment. Depending on the value of money owed to the employee, this could be for a term of up to 7 years' imprisonment.

We note that there appears to be a gap in the legislation in that the offence is only punishable by a term of imprisonment. This indicates only an individual could be prosecuted and sentenced. The previous versions of the Bill referred to the offence being punishable by fine of up to \$5,000 and/or imprisonment up to 1 year for an individual, or to a fine of up to \$30,000 in any other case (for example, where the defendant is a company). However, this provision was removed, and the offence now seems only subject to the punishment for theft generally. Therefore, we are not certain of how this could be applied to a company, and if so, what the punishment would be.

Further, the defence of “*reasonable excuse*” will need to be developed in the Courts. It is understood from the debate on the Bill in Parliament that the offence is not intended to capture mistakes, payroll glitches or short-term cashflow problems. However, it arguably could capture situations where an employer becomes aware of a mistake in payments owed to an employee/employees, and despite knowing of this, they do not take steps to pay the money to the employee.

We anticipate there will be some prosecutions and developments in this area. Should this issue arise, you can contact us for advice.

### Disclaimer:

This newsletter is not intended as legal advice but is intended to alert you to current issues of interest. If you require further information or advice regarding matters covered or any other employment law matters, please contact **Dean Kilpatrick, Jane Taylor, Nick Mason, Deborah Hendry or Jane Freeman.**