No more reason to misunderstand facial recognition rules in Australia

In a recent determination,[1] the Australian Privacy Commissioner found that the retailer Kmart breached the Privacy Act 1988 (Cth) by using facial recognition technology (**FRT**) on tens of thousands of customers from 2020-2022 without proper transparency, consent or justification under a "permitted general situation". The breach occurred across 28 stores in a pilot program targeting refund fraud.

Like Bunnings previously,[2] the retailer failed to conduct a privacy impact assessment and meet the necessity and proportionality requirements under the Act.

It is not all bad news, however. This determination is not a ban. It clarifies how organisations can lawfully deploy FRT, as demonstrated by Foodstuffs North Island which recently received a positive regulatory appraisal for meeting similar requirements under New Zealand's Privacy Act 2020.[3]

The underlying message here is to have a privacy impact assessment completed by a qualified team.

Refund fraud

The FRT targeted refund fraud which is when a perpetrator returns goods never purchased or bought at lower prices and identifying persons of interest.

Understanding the scale of the pressing problem being addressed through intrusive technologies is essential for a compliance assessment. Unfortunately, the retailer's relevant statistics were [redacted] in the Commissioner's determination. However, the Commissioner found that the FRT detected minimal fraud compared to the projected losses.

The retailer sought to address stock loss without using conventional means which could impact customer experience. Upon policy reversal in 2024, the retailer reported increased customer aggression when requiring receipts for returns.

How did it work?

The FRT took 5-6 face images of every person entering the store or attending the returns desk, creating metadata stored in a "history database" containing everyone's faces. An "enrolment database" included persons of interest identified by staff based on suspicious CCTV footage or behaviour. The enrolment database was shared among all stores.

When a customer at the returns desk matched either database, staff could view CCTV footage of the customer entering the store. The reason for this is [redacted] but possibly to see if the customer arrived with or without an item. Staff were trained to use the FRT check for customers who requested a refund without presenting a receipt, individuals flagged as a person of interest and in two other [redacted] situations.

[1] Commissioner Initiated Investigation into Kmart Australia Limited (Privacy) [2025] AICmr 155 (26 August 2025) (link).
[2] OAIC's decision a warning re use of facial recognition technology, KHQ Lawyers, November 2024 (link).
[3] Inquiry into Foodstuffs North Island trial use of facial recognition technology, Privacy Commissioner, May 2025 (link).

Staff could mark a customer acting suspiciously. Once marked, the customer was flagged as "known" at each store visit. Staff could also log incidents based on suspicion. Any refusal of a refund to an enrolled person was logged with particulars.

The Commissioner noted that rather than detecting actual fraud, staff using FRT were forming a suspicion based on subjective opinions, potentially putting customers through unwarranted scrutiny, being suspected of conduct which they may not have engaged in and possibly discrimination based on race, gender and other characteristics.

Transparency

The facial images and generated metadata used for automated biometric verification constituted sensitive information under the Act. Transparency is an essential requirement under the Act. A failure to comply would have wider ramifications – for example, any evidence generated by the retailer's fraud detection system in contravention of Australian law would likely be inadmissible in court proceedings.[4]

Even the Police have a duty to tell motorists about speeding cameras but the retailer argued that, in relation to FRT, no notice was required for "unmatched" individuals because no personal information had been collected and that notifying "matched" individuals was not reasonable. The retailer seemed to operate under a fundamentally different interpretation of the Act. Its service provider's FRT Guide explicitly instructed staff that "*under no circumstances should any Team Members disclose or advise customer on the use of this technology*".

Alternatively, the retailer claimed that adequate notice had been provided through an entry sign which read "*This store has 24-hour CCTV coverage, which includes facial recognition technology*" and a privacy poster which failed to mention FRT, both implemented in late 2021 in some but not all stores. An updated privacy policy referring to FRT was published around that time. The retailer failed to comply with its own Minimum Standards policy provided by its parent company Wesfarmers.

The Commissioner explained what reasonable transparency steps should have looked like and the relative ease of implementing them.

Permitted general situations

The Act requires either a statutory permission or the individual's consent for collecting sensitive information and the collection must be reasonably necessary for the organisation's functions.

The retailer justified the FRT deployment under the unlawful activity "permitted general situation" pursuant to section 16A of the Act which says:

> *(a) the entity has **reason to suspect** that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in; and*
> *(b) the entity **reasonably believes** that the collection, use or disclosure is **necessary** in order for the entity to take **appropriate action** in relation to the matter.*

[4] Section 138, Evidence Act 1995 (Cth) or Evidence Act 2008 (Vic).

The Commissioner applies a textual and purposive interpretation of the Act, taking into account the public interest in protecting privacy, the need to balance privacy with organisations' pursuit of legitimate activities and other objects of the Act.

The Commissioner accepted that the retailer had reason to suspect refund fraud but found that it could not have reasonably believed that the data collection was necessary for taking appropriate action.

Appropriate action

The Commissioner agreed that detecting and preventing refund fraud and to identify persons of interest was "appropriate action". However, the retailer's perception of the term relied on biometric verification of all customers. The Commissioner suggested that "appropriate action" should not be defined in reference to a specific methodology in mind.

The retailer argued that if taking action can be considered "appropriate", then any data collection is necessary. The end justifies the means. The Commissioner disagreed, framing the question whether investigating refund fraud would be impossible without collecting every single customer's biometric data.

The Commissioner distinguished "appropriate action" from tools, interim steps and conveniences of FRT, which are not themselves appropriate action.

Necessity

Data collection is necessary if it is more than merely helpful, desirable or convenient. The Commissioner disagreed with the retailer's submission that FRT was the only practical means of managing refund fraud. An assessment of necessity includes consideration of **suitability**, **alternatives** and **proportionality**.

Suitability

The Commissioner accepted that a person can hold a reasonable belief of necessity "*without having qualitative proof to that effect*".

The retailer relied on its management's lived experience of stock loss and claims of limited alternatives. The stock loss numbers provided were [redacted] but according to the Commissioner not all attributable to fraud. In any case, the figures only seemed to confirm the FRT system's limitations. The FRT was only effective for 3 out of 5 fraud techniques and even then, the use cases suffered from significant limitations.

The Commissioner accepted that, at best, the FRT system was partially suitable. Fundamentally, staff using the system were forming subjective suspicions rather than actually detecting fraud. This further highlighted the system's limited suitability.

Alternatives

The Commissioner explained that necessity required an assessment of less privacy-intrusive alternatives. The retailer claimed that none existed. The Commissioner rejected the retailer's suggestion that alternatives should only be considered if they are equally effective and as compelling as the FRT system.

The retailer provided no evidence of project planning, assessment of alternatives or a privacy impact assessment. In its defence, the retailer referred to three [redacted] alternatives. The Commissioner disagreed that customer experience issues make alternatives ineffective, suggesting several alternatives (returns counter at the entrance, radio tags, robust returns policy, staff training) which could have been easily implemented.

Proportionality

Proportionality is inherent in "necessity" under the Act, balancing privacy intrusion with organisations' legitimate objectives based on qualitative and quantitative factors. Ultimately, the Commissioner found that the data collection was disproportionate.

The retailer argued that the collection was not disproportionate due to the nature of collection, limited retention, security and limited likelihood of harm. The Commissioner countered by pointing out that tens of thousands of customers had biometric data recorded to detect fraud allegedly committed by a small group of people. She highlighted possible harms including discrimination and surveillance, particularly for enrolled customers who were likely suspected of conduct they never committed.

Conclusion

The Act is not a new law. Proportionality has been discussed in Australia since at least 2010[5] and remains relevant for modern technologies like FRT.

Here are some of the key lessons from this determination:

- Privacy impact assessments are required by law.
- Availability of technology does not mean its deployment is always lawful.
- Necessity requires an objective assessment not unduly favouring business goals or an unfounded desire to benefit customers or protect staff.
- FRT use cases must be narrowly designed and well managed.
- Alternatives must be honestly considered. It is a mistake to eliminate all alternatives to justify FRT.
- Aspirational effectiveness of FRT is not enough but carefully managed, even if imperfect, pilot programs can be lawful.
- Groundless challenges of fundamental privacy concepts while investigated make for bad optics.
- Organisations need proper advice, and advice from a provider motivated by commercial goals might be counterproductive.

All this clarity should result in better FRT compliance in future. Organisations must be mindful of the Privacy Commissioner's new powers. The unlawful handling of the sensitive information of tens of thousands of people will likely attract a significant civil penalty in future. For more information, please see the Privacy Commissioner's FRT guide.[6]

Alexander Dittel is a Principal in **Data Privacy, Cyber and Digital** at KHQ Lawyers

[5] *WBM v Chief Commissioner of Police* [2010] VSC 219 (Kaye J).
[6] Facial recognition technology: A guide to assessing the privacy risks, OAIC, November 2024 (link).