SQUIRE PATTON BOGGS

Bunnings v OAIC

What You May Have Missed

Australia – February 2026

On 4 February 2026, the Australian Administrative Review Tribunal (Tribunal) handed down its decision in *Bunnings Group Limited and Privacy Commissioner* [2026] ARTA 130 (Decision). Even without the hype, privacy rulings are few and far between, so you can imagine the level of anticipation that greeted it.

As has been widely reported, the landmark Decision partially overturned the 2024 determination by the Office of the Australian Information Commissioner (OAIC). For the privacy community, the Decision provides a nuanced recalibration of how the "permitted general situation" exemption under the *Privacy Act 1988* (Cth) (*Privacy Act*) may apply, especially to emerging technologies.

Many readers will already be familiar with the Decision and will have read other updates on what it means for privacy professionals. So, we decided to sharpen our focus by providing practical lessons that you may have missed in the coverage so far – and that may help you to decide whether enhanced surveillance is an option for your business.

Lesson 1:

The OAIC's findings of noncompliance are important, but should be the easiest ones for an organisation to fix

Much of the coverage of the Decision emphasises that the OAIC was partly vindicated in its initial determination. Indeed, before identifying what makes the Decision so groundbreaking, even the OAIC emphasised that the Tribunal had affirmed its findings on Bunnings' contravention of Australian Privacy Principles (APPs) 1 and 5.

We agree that the Decision underscores the importance of good privacy governance. But for many, the "kicker" was whether facial recognition technology (FRT) was part of the menu of retailers' security options at all. Ultimately, the Tribunal found that Bunnings was entitled to collect sensitive (biometric) information without consent because Bunnings reasonably believed that FRT was necessary to take "appropriate action" against retail crime. The Tribunal's findings on this point were complex: among other things, it needed to explain what "reasonable belief" requires (more below) and support Bunnings' concept of "unlawful activity" – which covered repeat retail crime only and was much narrower than the OAIC's interpretation.

This was more involved than the Tribunal's response to whether Bunnings had taken reasonable steps to notify individuals under APP 5, or to implement appropriate practices, procedures and systems under APP 1, even if, in hindsight, it seems obvious that the size and scale of a Bunnings store meant that its efforts to notify – which included slimline entry notices and a single in-store poster – were insufficient in the circumstances.

On this basis, the OAIC was right, but about things that are not controversial. Privacy-mature organisations know that good governance looks better than this baseline and should include a privacy impact assessment and well-socialised policy for use at a minimum. If FRT is on the menu, then doing it right is critical – and the Decision emphasises that obligations under APP 5 apply regardless of any exemption to the usual rules on collection, use and disclosure of personal information.

Lesson 2:

As the term suggests, "reasonable belief" gives organisations flexibility beyond absolute fact

In assessing whether Bunnings held a "reasonable belief" under APP 3, the OAIC acknowledged that Bunnings was entitled to a subjective view, but this view had to be assessed against objective facts and circumstances. However, the OAIC appeared to treat "reasonable belief" as a requirement for proof, focusing its attention on outliers (like balaclavas and face masks) and not on evidence that Bunnings had adduced on how FRT had prevented recidivist activity within their stores.

The Tribunal took a more permissive approach, finding that it was "reasonably open" to Bunnings' believing that it had a problem with repeat offenders that FRT could address. Although other factors were relevant (like the "significant intrusion into privacy" that FRT involves), these were outweighed by protections implemented by Bunnings, such as close-to-instant deletion of unmatched biometric information. In this way, the Tribunal invites businesses to take a more holistic view of FRT and offers more flexibility in assessing whether alternative means of protection can achieve the same outcome. This is different from the OAIC, which held that FRT's "limitations" meant that Bunnings could never have reasonably believed that FRT was necessary. The Tribunal's approach stands closer to the New Zealand Biometric Processing Privacy Code, which offers agencies the right to conduct a limited trial of FRT before any requirement for biometric data collection to be "necessary" kicks in.

Lesson 3:

The Decision does not apply to all retailers – and, conversely, it may apply more broadly than customer-facing operations

The Tribunal was clear to distinguish the Decision – and Bunnings more generally – from other retailers' practices. It noted that Bunnings faces unique security challenges due to the "size of its stores, with multiple entry and exit points" and due to unique threats, such as the possibility of customers driving a vehicle into stores or using merchandise as weapons. This serves as a warning that while the Decision broadens the OAIC's takeaways on how FRT can be lawfully used in retail, any use does not apply equally and must always be subject to legal and operational scrutiny.

While many commentators have noted the above, not enough have flagged that the situation faced by Bunnings can manifest in many other ways. The OAIC noted in its original determination that the use of FRT at airports or sports stadiums "[has] a different purpose and risk profile" from the use in retail. However, some organisations are operating in spaces that pose similar (if not identical) challenges. For example, open-air markets take place in venues that span hectares – and market authorities must monitor not only customer behaviour but also that of stall operators, who can number in the thousands and work at times of day where physical security is low. Like Bunnings, these spaces are open to vehicles and to stall operators who wield potential weapons as part of their day-to-day work.

The Decision has left the FRT door ajar for organisations. While it remains an extremely high-profile and complex area of the law, we encourage our clients to consider whether other security use cases could fall within the conditions set out by the Tribunal.

Lesson 4:

The Tribunal's refusal to confine the meaning of "collection" is relevant in an AI context too

A pivotal, yet often overlooked, point is that the Tribunal's strict interpretation of "collection" applies to input vector sets too.

Bunnings argued that because FRT generated a mathematical "vector" (a string of numbers) rather than storing the facial image input from the CCTV system, it was not collecting "sensitive information" in the form of biometric data. However, the Tribunal held that the FRT and CCTV systems were, in fact, operating together – and that creating vectors from sensitive information is still a form of collection. By mathematically transforming a facial image into a vector, the entity keeps a record of the (original) biometric information.

This closes any perceived loophole for AI developers, who claim that processing data in a "black box" without saving a copy avoids the reach of law. The Tribunal has confirmed that if an organisation derives personal information from other data, they have "collected" it under the Privacy Act.

What Next?

We hope that the above information was helpful and gave you something different to think about. If we can support on any of your thinking, please do not hesitate to let us know.

Author

Tanvi Mehta Krensel
Partner, Sydney
T + 61 450 657 742
E tanvi.mehtakrensel@squirepb.com