Australian Government
Office of the Australian Information Commissioner

Bunnings determination

Use of facial recognition technology

Bunnings operated a facial recognition technology system in 63 stores in Victoria and New South Wales between November 2018 and November 2021.

The system, via CCTV, captured the faces of every person who entered the stores – likely hundreds of thousands of individuals. Individuals' facial images were compared against those of individuals Bunnings had enrolled in a database who had been identified as posing a risk, for example, due to past crime or violent behaviour.

Investigation

The OAIC's investigation focused on whether Bunnings had complied with Australian Privacy Principles (APPs) 3.3, 5.1, 1.2 and 1.3.

- APP 3.3 says an entity must not collect sensitive information unless the individual consents or an exception applies.
- APP 5.1 requires an entity to take reasonable steps to notify an individual, or make sure they are aware, of certain matters around the handling of their personal information.
- APP 1.2 requires an entity to take reasonable steps to implement practices, procedures and systems to ensure they comply with the APPs.
- APP 1.3 requires an entity to have a clearly expressed and up-to-date privacy policy.

Facial images and other forms of biometric information are sensitive information under the Privacy Act. Sensitive information has a higher level of privacy protection than other personal information.

Findings

The Privacy Commissioner found Bunnings interfered with the privacy of the individuals whose personal information and sensitive information it collected through its facial recognition technology system.

- Bunnings collected the sensitive information of individuals without their consent. (Exceptions under the Privacy Act did not apply.)
- Bunnings failed to take reasonable steps to notify individuals about the facts, circumstances and purposes of their personal information being collected, as well as the consequences for them if their personal information was not collected.
- Bunnings failed to take reasonable steps to implement practices, procedures and systems to ensure it complied with the APPs.
- Bunnings failed to include in its privacy policies information about the kinds of personal information it collected and held, and how it collected and held that personal information.

Outcome

The Privacy Commissioner made various declarations, including that Bunnings must:

- not repeat or continue the acts and practices that led to the interference with individuals' privacy
- publish a statement about the conduct
- destroy all personal information and sensitive information collected via the facial recognition technology system that it still holds (after one year).