



Pathways for collection of sensitive information via facial recognition in retail spaces (APP 3)

Operating a facial recognition technology (FRT) system involves the collection of a person's biometric template and biometric information for the purpose of automated identification. This information is the sensitive information of the individual from whom it was collected.

Entities must not collect sensitive information unless there is a lawful basis for doing so. This flowchart sets out a process that entities can follow in assessing whether there is a reasonable basis for collecting individuals' sensitive information via the operation of an FRT system at their premises.

This document only sets out the situations most relevant to FRT in physical retail settings. Entities who are seeking to understand collection obligations under the Australian Principles (APPs) more broadly should refer to [Chapter 3 of the APP Guidelines](#)¹. That chapter sets out a range of considerations relevant to APP 3 and includes a [larger flowchart](#)² addressing the collection of all solicited personal information (not just sensitive information).



Assumptions

As a tool specific to considering the lawful basis for collection of sensitive information using FRT under APP 3, this flowchart makes the following assumptions:

- Your entity is an organisation for the purposes of the Privacy Act (see '[What is an organisation?](#)³'), and you as the relevant decisionmaker are considering using FRT to identify individuals at the physical premises of your entity.
- Your entity will take appropriate steps to comply with all other obligations under the APPs in relation to its use of FRT. As set out in guidance on FRT, particular attention should be paid to assessing risks and implementing appropriate governance arrangements, notifying or ensuring individuals are aware their information has been collected, addressing the risk of error and bias, keeping information safe, and ensuring it is deleted when no longer needed for a valid purpose.
- The FRT system collects the information directly from each individual, unless a relevant exception applies (i.e. because it is unreasonable or impracticable to collect personal information only from the individual – see '[Collecting directly from the individual](#)⁴')
- Entities do not rely on this document alone in making decisions about FRT, and will refer also to the [Privacy Act](#)⁵, [APP Guidelines](#)⁶, and [OAIC guidance](#)⁷.

Is the information collected via FRT reasonably necessary⁸ for one or more of your entity's functions?

NO

YES

Is your entity intending to use consent⁹ as the basis for collecting sensitive information?

NO

YES

Will consent be obtained from each person, in way that is voluntary, informed, current, specific, and given by someone with capacity?

NO

YES

Is your entity authorised or required by law¹⁰ to use FRT to collect the information?

NO

YES

Is your entity proposing to collect the information in relation to serious threats¹¹ or unlawful activity/serious misconduct¹²?

NO

YES

1. Is it impracticable to obtain consent and you reasonably believe collection is necessary* to lessen or remove the threat?
and/or
2. Do you have reason to suspect unlawful activity or serious misconduct and you reasonably believe collection is necessary* to take appropriate action?

*for both 1 and 2, is your belief that collection is necessary and reasonable, taking into account **suitability, alternatives, and proportionality**?

NO

YES

Does another relevant APP 3.4 exception¹³ apply?

NO

YES

Is your entity collecting the information by lawful and fair¹⁴ means?

NO

YES

If you conclude that your entity may collect the information via FRT, ensure it will comply with all remaining obligations under the APPs in relation to the information it has collected.



STOP: Your entity is likely to be in breach of APP 3.3 by collecting sensitive information without a lawful basis.

Linked pages

1. <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information>
2. https://www.oaic.gov.au/_data/assets/pdf_file/0023/263408/APP3-Are-you-collecting-solicited-information-flowchart.pdf
3. <https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act/rights-and-responsibilities#:~:text=What%20is%20an%20organisation%3F>
4. [https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information#section-collecting-directly-from-the-individual:~:text=3.2%20and%203.3\).-,Collecting%20directly%20from%20the%20individual,-3.89](https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information#section-collecting-directly-from-the-individual:~:text=3.2%20and%203.3).-,Collecting%20directly%20from%20the%20individual,-3.89)
5. <https://www.legislation.gov.au/C2004A03712/latest/text>
6. <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-c-permitted-general-situations>
7. <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/facial-recognition-technology-a-guide-to-assessing-the-privacy-risks>
8. <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information#section-collecting-for-an-app-entity-s-functions-or-activities:~:text=that%20identifies%20individuals.-,Collecting%20for%20an%20APP%20entity%E2%80%99s%20%E2%80%98functions%20or%20activities%E2%80%99,-3.12>
9. <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-b-key-concepts#:~:text=naa.gov.au%3E.-,Consent,-B.37>
10. [https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-b-key-concepts#:~:text=6%20\(APP%206\).-,Required%20or%20authorised%20by%20or%20under%20an%20Australian%20law%20or%20a%20court/tribunal%20order,-B.131](https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-b-key-concepts#:~:text=6%20(APP%206).-,Required%20or%20authorised%20by%20or%20under%20an%20Australian%20law%20or%20a%20court/tribunal%20order,-B.131)
11. <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-c-permitted-general-situations#lessening-or-preventing-a-serious-threat-to-life-health-or-safety:~:text=to%20that%20APP.-,Lessening%20or%20preventing%20a%20serious%20threat%20to%20life%2C%20health%20or%20safety,-C.4>
12. <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-c-permitted-general-situations#lessening-or-preventing-a-serious-threat-to-life-health-or-safety:~:text=permitted%20general%20situation.-,Taking%20appropriate%20action%20in%20relation%20to%20suspected%20unlawful%20activity%20or%20serious%20misconduct,-C.14>
13. <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information#section-collecting-directly-from-the-individual:~:text=fair%20means%E2%80%99%20below.-,Collecting%20sensitive%20information,-3.31>
14. <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information#section-collecting-by-lawful-and-fair-means:~:text=or%20moral%20issues.-,Collecting%20by%20lawful%20and%20fair%20means,-3.80>