Australian Government

Office of the Australian Information Commissioner

Facial Recognition Technology: a guide to assessing the privacy risks

Office of the Australian Information Commissioner

29 July 2026

OAIC

Contents

Who is this guidance for?

This guidance sets out general considerations for entities that are considering using facial recognition technology (FRT) to undertake facial identification in a physical commercial or retail setting. It does not cover all privacy issues and obligations in relation to the use of FRT, rather it provides information about key issues that arise under the Australian Privacy Principles (APPs). Entities should consider this guidance together with the *Privacy Act 1988* (Cth) (the Act) and the Australian Privacy Principles guidelines.

This guidance has been updated to reflect a decision of the Administrative Review Tribunal in relation to the use of FRT by Bunnings Group Limited. A separate determination issued in August 2025 by the Privacy Commissioner against Kmart Australia Limited, concerning its use of FRT, remains under review in the Administrative Review Tribunal.

Key points

- FRT involves the collection of a digital image of an individual's face and the extraction of their distinct features into a biometric template. The biometric template is then compared against one or more pre-extracted biometric templates for the purpose of facial verification or identification.
- The Privacy Act is technology-neutral and does not specifically ban or permit the use of FRT. Entities can use FRT in accordance with the Act in certain circumstances, provided their use complies with the Australian Privacy Principles.
- Biometric templates and biometric information, including facial images, when used for automated verification or identification purposes, are sensitive information under the Act.[1] Sensitive information is generally afforded a higher level of privacy protection under the Act. The OAIC expects regulated entities to have a clear and lawful basis for their collection and use of personal and sensitive information, including for use in an FRT system.
- Entities considering using FRT should conduct a privacy impact assessment (PIA) to identify potential privacy impacts at the outset and, if proceeding with FRT, implement recommendations to manage, minimise or eliminate those impacts. This supports a privacy by design approach from the start in accordance with an entity's obligations under APP 1.
- As part of a privacy by design approach, it is expected that key principles be considered and appropriately documented before using FRT, including:
    - **Lawful basis for collection (APP 3)**
        - **Consent pathway -** personal information for use in FRT must only be collected with valid consent and when it is reasonably necessary and proportionate in the circumstances.

[1] *Privacy Act 1988* (Cth) s 6 (definition of 'sensitive information'); Bunnings Group Limited and Privacy Commissioner (Guidance and Appeals Panel) [2026] ARTA 130 (4 February 2026) [76] ('*Bunnings*').

  - **Exception pathways -** where consent is not the basis for collection, entities should carefully consider whether one of the narrow exceptions applies.

- **Transparency and notification (APP 5)** – APP entities need to take reasonable steps to notify or ensure individuals are aware about certain matters related to the collection of their personal information, regardless of whether that collection is by consent or under a relevant exception.
- **Accuracy, bias and discrimination (APP 10)** – APP entities need to ensure that the biometric information used in FRT is accurate and steps need to be taken to address any risk of bias.
- **Security of personal information (APP 11)** – APP entities who hold personal information, even if only briefly, must take reasonable steps to protect that information from misuse, interference and loss, and unauthorised access and disclosure. They also have a duty to destroy or de-identify that information when no longer needed for a valid purpose.
- **Governance and ongoing assurance (APP 1)** – APP entities who decide to use FRT need to have clear governance arrangements in place, including privacy risk management practices and policies which are effectively implemented, documented, and regularly reviewed.

This guidance applies to use of FRT for identification in physical spaces, such as a shopfront or commercial retail setting. Systems built for other purposes, such as age assurance, will operate differently, collect different types of information, and involve their own unique privacy considerations. The OAIC has developed separate guidance about the use of age assurance technology.

Part A: Accountability and ongoing assurance (APP 1)

An APP entity will need to take reasonable steps to implement practices, procedures and systems relating to its function or activities that will ensure compliance with the APPs and any binding registered APP code.[2] The exact steps that are reasonable for this purpose will differ for each entity and use of FRT – a number of relevant circumstances and examples of reasonable steps are available in the APP Guidelines.

Conducting a privacy impact assessment (PIA) as set out below provides a formal, structured, and documented process for considering privacy implications, and assist to identify systems, policies and procedures relevant to an entity's specific implementation of FRT. Additionally, the *Privacy (Australian Government Agencies – Governance) APP Code 2017* (Cth) requires Government agencies to conduct a PIA for all high privacy risk projects.

[2] APP 1.2(b).

Adopting a privacy by design approach – privacy impact assessments

There is very real community concern about the privacy risks associated with FRT. To manage this and other associated risks, entities should conduct a formal, structured and documented risk assessment prior to implementing FRT in any form. Conducting a PIA as part of this risk assessment process will support entities to consider the specific privacy concerns associated with FRT, and instil a 'privacy by design' approach to their implementation.[3]

For agencies, it is mandatory to conduct a PIA for all high privacy risk projects.[4] Projects have a high privacy risk when they involve new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals. Considering the nature of FRT, it is likely that projects implementing the technology will have a high privacy risk and will require the conduct of a PIA by the agency.

Undertaking a PIA is also considered a reasonable step to take under APP 1.2 to ensure an APP entity is complying with their privacy obligations.[5] A PIA is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact. A PIA demonstrates commitment to, and respect for, individuals' privacy and other associated human rights. The OAIC strongly recommends entities publish their PIA report, as a demonstration that the implementation of FRT has undergone critical privacy analysis.[6]

This guidance highlights some key privacy considerations for entities to consider before determining whether to use FRT and when undertaking a PIA in relation to an FRT system. FRT is highly intrusive to an individual's privacy. This means that negative privacy impacts will be identified as part of the privacy impact analysis in a PIA, which will need to be managed or mitigated if the entity decides to proceed with the use of FRT.

Undertaking a PIA before using FRT

- APP entities regulated by the Privacy Act should conduct a PIA for projects involving sensitive information such as FRT. The OAIC has identified 10 steps which should be considered when undertaking a PIA in relation to a new, or updated project. Further information on each step is available in the OAIC's PIA Guide.

Assessing privacy risks across multiple premises

Some entities may wish to operate an FRT system across multiple premises, or to operate multiple separate FRT systems. Many of the factors set out in this guidance which are relevant to decisions about FRT, and which will need to be considered in a privacy risk assessment or PIA, respond to circumstances that can vary significantly between individual premises. Entities considering using FRT

[3] See OAIC, Privacy by design.

[4] *Privacy (Australian Government Agencies – Governance) APP Code 2017* (Cth) Part 12.

[5] For example, see *Bunnings* [226].

[6] Where commercial or security constraints limit the publication of a full report, the OAIC recommends entities still publish a summary or edited version.

across multiple locations therefore need to consider whether there are differing features that affect the issues covered in risk assessments, PIAs, and decisions to collect sensitive information.

A single risk assessment process could cover multiple premises which are substantially similar. When considering whether to do so, entities should think about how the set of locations under consideration was chosen, and actively consider whether there are any locations (or sub-sets of locations) that have specific features that warrant a separate assessment, or consideration of additional relevant factors beyond those covered in the general assessment. Examples of differences that could necessitate separate or additional assessments could include:

- The purpose for which FRT is being proposed – for example to address a safety problem with serious threats, compared to addressing retail fraud.
- When using FRT to address serious threats or unlawful conduct – the particular safety and threat profile of each store.
- Physical differences in the premises such as relative size, whether they are free-standing or within a shopping centre or mall, whether vehicles can enter, and whether there are one or multiple entrances.
- Differences in the types of business carried out or goods sold in the premises.

Thinking about these differences between premises will also help to identify the factors that will be particularly relevant in each risk assessment. Entities that choose to assess use of FRT across multiple premises as part of a single process should keep records noting how the set of premises was chosen and why they are considered sufficiently similar, and incorporate these into the report produced about their risk assessment or PIA.

If considering operation of an FRT system across multiple premises, entities should also think about the changes that might be required to comply with the various requirements set out throughout this guidance. For example, there is a difference between collecting and storing sensitive information for the purpose of keeping staff safe in one location compared to across a large chain. This would require changes to the information provided to customers about FRT in collection notices and privacy policies. Entities should also consider how personal information will be kept secure if it is being transferred between different locations, and how to ensure all copies are destroyed or de-identified when no longer required.

Implementing PIA findings

Compliance with APP 1.2 is not limited to conducting a PIA. Entities should consider how the appropriate systems, policies and procedures identified in the conduct of a PIA will be implemented in practice. An APP entity should be able to demonstrate the steps it has taken to ensure compliance in line with the considerations set out in this guidance, and that its practices, procedures and systems are regularly reviewed and updated.

FRT topics in policies and procedures

In the context of FRT, the topics addressed in policies and procedures should include, but are not necessarily limited to:

- How the FRT system collects, uses, holds, discloses and deletes personal information
- The circumstances in which the FRT system can be used
- Controls on staff access to the FRT system and the referenced database, with training requirements for relevant staff and procedures for revocation of access for those who no longer require it
- The process for enrolling and reviewing images in the referenced database
- The process for assessing positives and false positives
- A retention and destruction protocol for any biometric information collected
- The process for providing individuals access to personal information held about them,[1] correcting incorrect personal information,[1] and handling complaints
- The keeping of accurate records and documentation about the use of the FRT system, and
- Systems to review the efficacy of the FRT system and ensure implementation of the relevant policies and processes.

Third party FRT providers

Some entities may seek to engage a third-party provider to install or operate an FRT system on their behalf. Where this is the case, it remains the responsibility of the entity engaging the third-party to ensure that the FRT system is compliant with the Privacy Act. Before deploying a third-party designed or operated FRT system, entities should make inquiries to properly inform their own PIA. This is particularly important if the third-party is located offshore as you may be held liable for the acts of those third-parties. Entities should consider:

- Requesting relevant documentation, such as the third-party's privacy policy, information security policy and data breach response plan.
- Conducting due diligence, for example investigating any past security incidents associated with the product or service.
- Including contractual arrangements with your service providers to include terms to deal with specific obligations about the handling of personal information and mechanisms to ensure the obligations are being fulfilled (such as review and audit clauses).
- Conducting periodic reviews of the personal information handling requirements of the arrangements.
- Keeping detailed records of your arrangements with the third-party to maintain an audit trail and ensure you know what personal information the FRT system collects and holds.
- At the end of the contract, asking the third-party to confirm that they have deleted any personal information in accordance with the contract terms.

Just as with self-controlled implementations, due diligence for third-party operated FRT systems should not amount to a 'set and forget' approach. To ensure compliance with privacy obligations, entities should conduct regular reviews of the methods deployed to ensure they are configured appropriately, and that their ongoing use remains reasonable and necessary in the circumstances.

FRT in privacy policies

APP entities will also need to have a clearly expressed and up to date privacy policy about how they manage personal information, such as biometric information collected using FRT.[7] This needs to be regularly reviewed and updated to ensure it accurately reflects the entity's information handling practices. An entity's privacy policy should make specific reference to its use of FRT: it is not sufficient to state generally that video surveillance is in use, or that images are captured by use of cameras in stores.[8]

The privacy policy should provide the relevant information in a way that is easy for individuals to understand and navigate.[9]

Automated decisions

From 10 December 2026, the Act will require APP entities to include additional information in their privacy policy where they have arranged for a computer program to use personal information to make a decision, or do something substantially and directly related to making a decision, that could reasonably be expected to significantly affect the rights or interests of an individual.[10]

In considering the application of this obligation in the context of FRT, entities must consider whether their use of FRT may result in decision making which significantly affects individual's rights or interests. The effects from an APP entity's use of FRT must be more than trivial and must have the potential to significantly influence the circumstances of the individual concerned, regardless of whether the individual is adversely or beneficially affected.

For example, APP entities may consider factors such as whether the use of FRT results in limitations on individuals' access to essential goods and services or premises in a manner which significantly affects their rights or interests. APP entities should also consider the impact of any decisions made by FRT on persons experiencing vulnerability including children.

Entities should consider

- Have you conducted a comprehensive privacy impact assessment?
- What governance arrangements do you have in place? Some examples include designated privacy officers and regular reporting to the entity's governance body.
- How is the effectiveness of privacy risk management practices and policies being assessed?
- Do you have clear processes in place to ensure you are handling personal and sensitive information in accordance with your legislative obligations?

[7] APP 1.3.

[8] See e.g., *Bunnings* [230]-[233].

[9] See APP Guidelines [1.8].

[10] The OAIC is developing expanded guidance on the new APP 1 obligations that will commence from 10 December 2026 under amendments made by the *Privacy and Other Legislation Amendment Act 2024* (Cth). An Issues Paper on this topic was released for public consultation on 18 May 2026.

- Are you delivering training on privacy, risk management and other practices and policies to employees? Training should be documented and conducted periodically to refresh and update employee's knowledge on emerging privacy issues.
- Have you clearly outlined how employees are expected to handle personal and sensitive information?
- Do reporting mechanisms exist to ensure that employees are routinely informed about changes to practices and policies?
- Are you regularly reviewing and updating your privacy policy to ensure that it reflects your information handling practices?
- Is there an adequate level of human control or oversight over the FRT?
- Are you undertaking periodic audits of the effectiveness and necessity of using the FRT?
- Given the rapid pace of FRT advancements, are privacy risk management practices and policies flexible and adaptable to changes in technology?
- Have you developed a data breach preparation and response plan that can be relied on the event of a cyber security incident? If you are relying on a third-party hosted FRT system, consider who will be allocated responsibility for meeting legislative requirements. For example, if the biometric information is jointly held, who will be responsible for complying with the Notifiable Data Breaches scheme in the event of a data breach and handling complaints?
- Are there processes that allow individuals to easily access and correct their personal information? You must respond to a request for correction within a reasonable period after the request is made. In most cases, a reasonable period will not exceed 30 calendar days.
- If you are relying on a third-party hosted FRT system, have you obtained sufficient information to inform your privacy risk management practices and policies?

Part B: Lawful basis for collection (APP 3)

FRT requires the collection of biometric information to function. Even where a system captures and discards biometric information and/or biometric templates at a rapid pace, the practice amounts to a collection of personal information that must be consistent with the Privacy Act – there is no minimum temporal threshold for collection.[11] Images are 'collected' for inclusion in a record even where they are stored only in the random access memory (RAM) of a computer possessed or controlled by an entity, and not in persistent memory.[12]

Acts or practices, such as the deployment of FRT, that involve the collection of sensitive information must generally meet the following requirements (together referred to in this guidance as "**the consent pathway**"):

1. The collection of sensitive information must be 'reasonably necessary' for one or more of the entity's functions or activities or, for government agencies, directly related to one or more of the agency's functions or activities; and
2. The individual must consent to the collection.[13]

There may be practical difficulties with meeting the requirements of the consent pathway to use FRT in spaces typically open for members of the public to enter. The nature of FRT means that it is not often practical to obtain valid consent from individuals whose biometric information might be captured. Entities which are not able to meet the requirements of the consent pathway, including because obtaining consent is unreasonable or impracticable, must not use FRT unless an exception applies.[14] The possible exceptions are set out in APP 3.4.[15] The ones that are likely to be most relevant to APP entities considering using FRT in a shopfront/retail setting are:

1. Collection of information required or authorised by or under an Australian law or an order of an Australian court or tribunal ('**the authorised by law pathway**'),[16] or
2. Where a 'permitted general situation' applies ('**the permitted general situation pathway**').[17]

APP 3.4 also includes other exceptions that are less relevant to this guidance, including in relation to collection by enforcement bodies, collection in permitted health situations, and collection of information relating to the members of non-profit organisations. For information on these exceptions refer to Chapter 3 of the APP Guidelines.

Regardless of the 'pathway' relied on as the lawful basis for collection of sensitive information, entities bear a range of other obligations under the APPs when deploying FRT. Collected information should be limited to what is reasonably necessary and collection should be done by lawful and fair means. Further relevant considerations particularly relevant to FRT are set out in the other sections of this guidance.

---

[11] *Bunnings* [59]

[12] *Bunnings* [64]-[65].

[13] APP 3.3(a)

[14] APP 3.3(b)

[15] See also Australian Privacy Principle Guidelines, Chapters 3; C ('*APP Guidelines*')

[16] APP 3.4(a).

[17] APP 3.4(b). See APP Guidelines Chapter C.

The Consent Pathway

Where sensitive information is to be collected based on individuals' consent, the collection must be **both** reasonably necessary, and subject to valid consent being obtained.

Due to the practical difficulties with obtaining valid consent from each individual in spaces generally open to the public, the consent pathway is most likely to be applicable to use of FRT where entities are able to make contact with each individual before their physical attendance at a location. For example, entities that require each customer to make a booking or obtain a membership in advance of their physical attendance may have the opportunity to seek consent that meets the requirements set out below.

Reasonably necessary

The APP Guidelines provide information about when the collection of personal information is reasonably necessary for one or more of an entity's functions or activities, or directly related to one or more of an agency's functions or activities.[18] It is up to an entity to justify that the collection is reasonably necessary. The fact that collecting personal and sensitive information via FRT is available, convenient, affordable or desirable should not be relied on to establish that it is necessary to collect the information.

Entities should consider

Is the collection of biometric information reasonably necessary to perform a particular function or activity? 'Reasonably necessary' depends on factors including whether the collection is proportionate, which involves balancing the privacy impacts resulting from the collection against the benefits gained, with reference to the relevant activity. Factors to consider include:

- What is the primary purpose of collecting the information?
- Can the biometric information be collected, used, stored and secured in a more privacy-respecting way in undertaking a function or activity?
- Can you undertake the function or activity without collecting the biometric information?
- Can the purpose be achieved by less intrusive means? Have you considered other alternative means?
- Have you identified and assessed the benefits and privacy risks? Do the benefits to be achieved clearly outweigh the privacy risks, and why?
- Is there a clear public interest in using FRT? Examples may include to lessen or prevent a serious threat to public health or safety.
- Would an individual reasonably expect FRT to be used in the circumstances? Will the use of FRT lead to unjustified adverse effects, such as unjust discrimination?

[18] APP Guidelines [3.12]-[3.30].

Obtaining consent

To obtain valid consent, certain elements will need to be met. These include:

- The individual being adequately informed before giving consent
- The individual giving consent voluntarily
- The consent being current and specific, and
- The individual having the capacity to understand and communicate their consent.[19]

Merely having signage or notice about the use of FRT in and of itself, will not generally be sufficient to show that an individual has consented to the use of FRT. This is because the information is sensitive information, and all four elements of consent are unlikely to have been satisfied.

Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the entity seeking consent. Generally, implied consent should not be relied on when collecting sensitive information, including biometric information. The mishandling or inappropriate use of biometric information can have adverse consequences for an individual or those associated with the individual. It can also cause humiliation, embarrassment or undermine an individual's dignity.[20]

Opt-out mechanisms are a type of implied consent. It is only appropriate to infer consent from an opt-out mechanism in very limited circumstances.[21]

Entities should consider

- How will you be transparent and provide information about the use of FRT to individuals to ensure they are able to provide informed consent?
- Have you considered the four key elements of consent?
- How will consent be obtained from individuals who have particular needs, such as individuals from a non-English speaking background and children?
- If biometric information is sourced from a third-party, has the third-party collected it lawfully and do they have authority to disclose it to you?
- If an individual does not consent to the collection of their biometric information or withdraws their consent, is an alternative process available which will not result in detriment to the individual?

[19] APP Guidelines [6.17].

[20] APP Guidelines [B.144].

[21] APP Guidelines [B.41]–[B.43].

Authorised by law pathway

APP entities are not required to seek consent to collect sensitive information where that collection is required or authorised by or under an Australian law or a court/tribunal order.[22] The APP Guidelines provide information about when a law or order 'requires' or 'authorises' collection.[23] Collection of sensitive information on the basis of a legal obligation or authority should be limited to the information that is reasonably necessary to fulfil an entity's obligation under that law or order. In addition, entities should ensure their handling of the information is proportionate to the aim of fulfilling the legal obligation.[24] As with the consent pathway, collection where authorised by law should also be limited to what is reasonably necessary for an entity's functions or activities, or for an agency, directly related to functions or activities.[25]

A law will only authorise collection of sensitive information using or for use in FRT where the law is explicit about the collection or authorises a practice that directly entails using FRT.[26] Collection is not authorised just because a law or order does not explicitly prohibit collecting the information using of FRT.[27]

For example, in South Australia venues with licences to operate more than 30 gaming machines are required to implement an FRT system for the purpose of excluding persons barred from gambling in a venue.[28] The South Australian law also authorises licensees who are not strictly required to implement FRT to do so to support responsible gambling obligations.[29]

By contrast, a law generally requiring venues to take steps to exclude barred patrons from areas with gambling machines, without expressly requiring or authorising use of FRT, or directly entailing its use, would not provide a lawful basis for collection.

Entities should consider

- What is the law or legal order that explicitly requires or authorises you to collect the sensitive information involved in operating an FRT system?
- How will you comply with any limits or conditions that are imposed on the requirement or authorisation for you to operate the FRT system?
- Is the information you collected limited to that which is reasonably necessary, for example to comply with the requirements imposed by the law or order?

[22] APP 3.4(a).

[23] APP Guidelines [B.131]-[B.140].

[24] APP Guidelines [3.12].

[25] APP Guidelines [3.12]-[3.30].

[26] APP Guidelines [B.134].

[27] APP Guidelines [B.135].

[28] *Gaming Machines Act 1992* (SA) Sch 1 para (ka). The facial recognition system must be one authorised by the Liquor & Gambling Commissioner (SA) under *Gaming Machines Act 1992* (SA) s 40D and operated in accordance with *Gaming Machine Regulations 2020* (SA) r 28, and any conditions affixed to the gaming machine licence.

[29] Gambling Administration Guidelines: Facial Recognition Systems – Gaming Machine Licence (22 July 2021) (SA) 4(3).

Permitted general situation pathway

There are seven permitted general situations set out in section 16A of the Act. The first two, relating to serious threats and unlawful activity, are the most likely to be relevant to the deployment of FRT in retail and commercial environments.[30] These two permitted general situations are separate but closely related and involve overlapping considerations. It is possible that an FRT system may collect sensitive information for the purposes of both at once – for example where FRT is used to address a serious threat of violence in stores, where the conduct giving rise to the threat is a criminal offence. The elements involved in each permitted general situation in relation to collection are set out below.

Permitted general situation 1 – Serious threat	**Permitted general situation 2 – unlawful activity or serious misconduct**
(a) It is unreasonable or impracticable to obtain an individual's consent to the collection, and	(a) there is reason for the entity 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 collecting information for FRT reasonably believes it is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.	(b) the entity reasonably believes that the collection is necessary in order for it to take appropriate action in relation to the matter.

Permitted general situation 1 - Serious threat

The 'serious threat' permitted general situation applies where an entity collects biometric information or biometric templates via FRT under a reasonable belief it is necessary to prevent or lessen a serious threat, in circumstances where it is unreasonable or impracticable to obtain individuals' consent to collection of their personal information. An entity should be able to point to one or more clear reasons that make it unreasonable or impracticable to obtain individuals' consent to the collection of their sensitive information by an FRT system.[31]

APP entities seeking to use FRT on the basis of this permitted general situation should also be able to clearly identify and articulate the threat being addressed, and why it is serious. In a retail setting, information relevant to assessing whether you believe it is necessary to collect personal information to lessen or prevent a serious threat could include evidence about the nature and severity of the threat and the security environment of your shopfront/retail setting. You should consider if there are relevant factors such as:

- Threatening behaviour that may cause serious psychological harm or, if the threats were carried out, serious physical harm.

[30] The full table of permitted general situations is set out at s 16A of the Privacy Act. For guidance on the application of each permitted general situation, refer to APP Guidelines Chapter C: Permitted general situations
[31] Relevant considerations are set out in the APP Guidelines [C.6].

- Incidents involving acts of physical violence or aggression.
- Threats that involve weapons such as knives, tools, syringes, and firearms.
- Specific features of your shopfront environment that could change the nature of the threat and appropriateness of FRT, such as multiple entry/exit points, or vehicles driving inside the store.

Permitted general situation 2 - Unlawful activity or serious misconduct

For the second permitted general situation to apply an entity must have reason to suspect unlawful activity or serious misconduct. This does not require the entity to actually form an opinion that the activity or misconduct has been, or is being, engaged in.[32] Entities should be able to demonstrate the reasonable basis of their suspicion.

Where that reasonable suspicion exists, FRT could be used to collect biometric information or biometric templates if an entity reasonably believes it is necessary in order to take 'appropriate action' in relation to the suspected activity or misconduct.

Appropriate action should be proportionate to the severity of the suspected unlawful activity. Appropriate action could, for example, include investigating an unlawful activity and reporting the matter to the police.[33] However, using FRT to collect sensitive information of every individual as part of that investigation would only be appropriate if it is necessary to address very serious unlawful activity, such as repeated acts of theft, violence and abuse.

If FRT is used, entities should ensure their FRT system does not collect more than is needed to take that action and consider whether a more constrained use of FRT could be implemented.[34] Constraints could include electing a technical implementation that collects and retains a lower volume of sensitive information, and using FRT only in particular parts of a store.

Reasonable belief and necessity for permitted general situations

The permitted general situations above both require an entity to believe its collection of information by use of FRT is necessary for a particular purpose. There must be a reasonable basis for the belief held by the entity, and not merely a genuine or subjective belief.[35] It is the responsibility of an entity relying on the permitted general situation pathway to be able to justify that its belief in a relevant circumstance was reasonably formed. This requires consideration of the objective facts and circumstances, and whether these would induce the relevant belief about the necessity of FRT in a reasonable person.[36]

---

[32] *Bunnings* [105]-[106], referring to consideration of the phrase 'reason to suspect' in the context of ASIC corporations legislation regulation by Rofe J in *Provide Nominees Pty Ltd v Australian Securities and Investments Commission* [2024] FCA 303 [43].

[33] APP Guidelines [C.20].

[34] See APP Guidelines [3.26].

[35] APP Guidelines [C.8]; *Bunnings* [111].

[36] *George v Rockett* (1990) 170 CLR 104 112, 116. See also *Seven Network v Australian Competition and Consumer Commission* (2004) 140 FCR 170 182.

While 'necessary' is not defined in the Act, the APP Guidelines indicate that the term requires something more than the collection, use or disclosure being merely helpful, desirable or convenient.[37]

When considering whether they reasonably believe it is necessary to collect information in the context of a permitted general situation, entities should consider:

a. the **suitability** of collecting the information captured by the particular FRT system under consideration, including the efficacy of that collection in addressing the relevant threat or unlawful activity
b. the **alternatives** to collecting the personal information that are available to the entity to address the threat or activity (including alternatives that still involve collection of personal information but are less intrusive or more proportionate), and
c. whether collecting the personal information by use of FRT is **proportionate** to the impact to individuals' privacy.[38]

The purposes for which FRT may be necessary in permitted general situations are narrowly constrained. Assessing the reasonable necessity of FRT through the factors of suitability, alternatives, and proportionality requires entities to have regard to the specific nature of the serious threat and/or unlawful activity or serious misconduct they seek to address, the context in which that conduct occurs, and features of the proposed FRT system they propose to use.

Suitability

The suitability of an FRT system collecting personal and sensitive information concerns not just whether the system is effective at accurately identifying matched individuals without making errors, but also whether use of the system is more broadly effective in dealing with the threats, unlawful activity or serious misconduct an entity is dealing with.

Entities should consider whether an FRT system, and in particular whether the specific system proposed for implementation, will be effective in this regard, and how this can be measured. As part of this process, entities should also consider the limitations of the FRT and associated security systems. For example:

- technical or practical limitations that mean that there is limited opportunity to take effective action even where a positive match is made identifying an individual of concern.
- environmental factors in a physical space, such as lighting and camera positioning, could limit the ability of a system to accurately match individuals' faces or associated biometric templates.
- an entity may be aware of strategies commonly employed by malicious individuals that in practice frustrate the effectiveness of the FRT in identifying them.

As addressed below in relation to accuracy (APP 10), as well as accountability and ongoing assurance (APP 1), the effectiveness of FRT is not a one-time assessment. Entities should have processes in place that ensure it can measure and continue to review the effectiveness of an FRT system while it is in operation.

Alternatives

The test is not whether there is an alternative system that could be equally effective or achieve strictly like-for-like outcomes to collecting the personal information captured by use of FRT. Instead, entities should give genuine consideration to whether there are less privacy-intrusive methods that could be

[37] APP Guidelines [C.8].

[38] *Bunnings* [162]-[165].

practically and effectively deployed as a means towards achieving the same outcome.[39] An entity that considers there is not an appropriate alternative to use of FRT should be able to articulate why less privacy-intrusive methods are not practical or effective.

Whether there are alternatives available to FRT that are less privacy intrusive will necessarily depend on the context and circumstances of an entity, and the nature and severity of the problem the entity seeks to address. Entities should consider whether their operating environment has unique features that necessitate use of FRT, as opposed to some other security response. Relevant factors include:

- The size of the retail or commercial premises
- Whether there are multiple entry and exit points
- The manner in which customers can access the premises – for example by foot, driving a vehicle, or a combination of these
- Whether the environment would enable or exacerbate the seriousness of unlawful conduct such as by making things that can be used as a weapon readily accessible.

Alternatives to using an FRT system to monitor for safety and security concerns may include (for example):

- Quality CCTV coverage
- The deployment of security guards, including covert security guards
- Training employees in dealing with safety and security issues
- Taking legal action to restrict known repeat offenders from entering a store, such as seeking a workplace protection order (in jurisdictions where these are available)
- Close engagement with law enforcement.

Proportionality

Entities need to balance the privacy impacts against the benefits provided by the use of an FRT system.

Benefits gained from the use of FRT may be proportionate where it is implemented to effectively address serious unlawful activity – such as where there is evidence of a significant level of theft and violence being perpetrated by repeat offenders, and it has been assessed that the FRT system will be effective at reducing this.[40]

However, it may conversely be the case that the benefits gained from the implementation of an FRT system do not outweigh the privacy impacts. Not all types of threat, unlawful activity or misconduct will necessitate use of FRT, and the benefits gained will depend on the particular circumstances and FRT system that is proposed to be implemented.

For example, collection of every individual's sensitive information would not be a proportionate action to take to address less serious activity that does not involve violence or patterns of repeated misconduct. Similarly, use of an FRT system that is only partially effective at addressing targeted offending conduct, and/or which is effective at addressing only a narrower subset of targeted conduct, might not be proportionate, because it provides limited benefits that do not proportionately outweigh the privacy impacts.

[39] See e.g. *Bunnings* [161].

[40] See e.g. *Bunnings* at [93], [95] and [96].

Entities should consider

Permitted general situation 1:

- Would it be reasonable to obtain each individuals' consent to your collection?
- What is the threat, and what makes it serious?
- What are the features of the threat and your security environment that lead you to believe collection of information by FRT is necessary to prevent or lessen that threat?

Permitted general situation 2:

- What unlawful activity or serious misconduct do you suspect is, has been, or may be occurring? What is the reason for that suspicion?
- Why do you believe it is necessary to collect each individual's sensitive information to address the activity or misconduct?

Both – for the purpose of assessing reasonable belief that the collection is necessary:

- Is collecting sensitive information by operating an FRT system a suitable response to the activity or conduct? Is the processing of that information by the FRT system accurate? How does it address the issue that gave rise to the permitted general situation?
- Is there a reason other security or safety measures are not an appropriate or effective alternative to collecting individuals' sensitive information?
- What are the benefits of you collecting personal and sensitive information by operating your FRT system? How can you quantify those benefits, and do they outweigh the serious privacy impacts involved?

Case study – FRT in the Bunnings retail environment

The use of FRT under a permitted general situation was considered in a decision of the Administrative Review Tribunal (ART) in relation to Bunnings Group Limited. While entities must consider their individual circumstances carefully, the decision of the ART is a useful case study about how the factors relevant to necessity and proportionality apply in a commercial retail setting.

Bunnings operated an FRT system to address significant problems it was facing with violence and theft. Bunnings argued its use of an FRT system fell within a permitted general situation. The issue Bunnings sought to address constituted both a serious threat of harm and unlawful activity. In Bunnings' circumstances, it was agreed that it was impracticable to obtain the consent of every customer whose biometric information would be collected.

Suitability

Bunnings proved its use of FRT was effective at addressing the problem of retail crime and violence because the identification of known offenders enabled staff to be alerted and to remove such individuals from the store. When this was done proactively, it reduced the number of violent incidents, compared to confronting individuals only after they had engaged in theft or threatening conduct.[41]

While the known offenders that could be identified by the FRT system were a relatively small proportion of the total number of offenders, the system regardless provided the benefit of avoiding serious potential incidents, and made staff feel safer.[42] Bunnings also used human intervention to verify matches identified by the FRT system. This adequately mitigated the risk of acting on a false positive match.[43]

Alternatives (limited by unique characteristics of Bunnings stores)

The security environment in which Bunnings operates is 'significantly different from that of most other retailers'.[44] This created unique challenges for prevention of theft and threatening situations and constrained the availability of effective alternatives to FRT. Its stores were large and had multiple entry and exit points, including allowing customers to drive vehicles into the store. Many of the readily accessible products sold in Bunnings stores (such as an axe, screwdriver, or drill) could be used as a weapon by an offender.

In that setting, security experts assessed there were no alternate security controls available to Bunnings which would be likely to effectively and consistently identify repeat offenders.[45] The ART found that:

> 'The reason why FRT was effective was because it could survey the facial features of nearly every person who entered a Bunnings store. Less privacy-intrusive alternatives could not achieve the same outcome in terms of dealing with repeat offenders. No other security control could identify repeat offenders in the way that FRT did for the purposes of monitoring them and preventing further offending.'[46]

[41] *Bunnings* [137]-[141].

[42] *Bunnings* [142]-[143].

[43] *Bunnings* [153].

Proportionality

Bunnings had records showing it had a very serious problem involving organised retail crime and serious abuse being perpetrated by repeat offenders, with staff in a Bunnings store experiencing threatening or abusive behaviour at least every two to three days.

Some features of the specific FRT system implemented by Bunnings that informed the proportionality of its use to the benefits it provided in addressing the serious problem included that:

- Collected information was stored only briefly (for a few milliseconds) before being permanently deleted when there was no match[47]
- The design and security arrangements of the system meant there was a low probably that collected information would be subject to a cyber attack or on-sold to a third-party[48]
- It was not possible to reconstruct an individual facial image from the biometric template generated by the FRT system[49]

Due to the high severity of the safety issues faced by Bunnings, these design features 'limited the impact on privacy so as not to be disproportionate when considered against the benefits of providing a safer environment for staff and customers in Bunnings stores.'[50]

Part C: Transparency and notification (APP 5)

APP entities are required under the Act to manage personal information in an open and transparent way.[51] As an important measure for transparency, APP 5 requires APP entities to take reasonable steps to ensure that an individual is aware of certain matters when the entity collects their personal information. This is particularly important in the context of FRT because there are many complexities surrounding the technology that can impact an individual's ability to understand how their personal information is collected and handled.

Reasonable steps to notify individuals

APP entities that are collecting personal information must take reasonable steps to either notify the individual of certain matters, or ensure the individual is aware of those matters.[52] The reasonable steps required for each of the matters will depend on the circumstances, but more rigorous steps may be needed when collecting sensitive information, such as biometric information.

---

[44] *Bunnings* [161].

[45] *Bunnings* [159].

[46] *Bunnings* [161].

[47] *Bunnings* [167]-[168].

[48] *Bunnings* [171]-[172].

[49] *Bunnings* [170].

[50] *Bunnings* [172].

[51] APP 1.1.

[52] APP 5.1; the matters are listed under APP 5.2. See also APP Guidelines [5.8]-[5.33].

Reasonable steps need to be taken to notify all individuals whose sensitive information will be collected. This includes every person whose face is captured by an FRT system, including non-matches, not just those whose information is stored in a database for positive matching. This is the case even where collected information is rapidly disposed of, for example where information is briefly stored in system memory and deleted after the system finds no match with a stored biometric template.[53] You should also consider the steps that are reasonable to notify individuals when you collect their personal information to store in a database, for the purpose of later identifying them using an FRT system.

The requirement to take reasonable steps under APP 5 applies regardless of whether the FRT system collects personal information in reliance on the consent pathway or an exception. It is also separate to the requirement to provide information in a privacy policy under APP 1.3.[54]

Some factors that are particularly relevant when considering what steps would be reasonable to take for notification in relation to FRT include:

- that the information being collected from each individual is sensitive information
- how long a person's sensitive information is retained, and whether it is possible to recover or re-identify the information that was intended to be disposed of
- that the information can result in detriment to an individual, such as the potential for a false positive result and unjust discrimination[55]
- that individuals may not otherwise be aware their sensitive information is being or will be collected by an FRT system (as opposed to traditional video surveillance), even where they are aware a camera is capturing images in the store.

Form of notification

Reasonable steps must be taken to notify individuals of a range of matters set out in APP 5.2 and the APP guidelines.[56] The steps that are reasonable for each matter may be different, and it may be reasonable for an entity to notify some but not all of the APP 5 matters.[57] Steps taken do not have to be identical for each matter, and entities should consider a range of methods of notification.

At a minimum, steps should specifically and positively identify where an FRT system is in use, and for what purpose.[58] A generalised notification about use of surveillance is not sufficient to meet the requirements of APP 5 when using FRT.

Where it is not reasonable to display particular information on signage (for example, because excessive detail would limit accessibility and the salience of the key matters addressed by the signage), entities should take other steps to ensure individuals are otherwise made aware. For example, a collection notice about the use of FRT might indicate that additional relevant information

[53] *Bunnings* [64]-[66].

[54] APP Guidelines [1.8]-[1.14]. In some limited circumstances where it is not reasonable to notify the full range of required matters, an APP entity might consider directing individuals to relevant sections of its privacy policy (and in doing so consider whether the policy sufficiently covers the APP 5 matters as they relate to the particular use of FRT) – see APP Guidelines [5.6].

[55] The potential for a false positive result, even where low and subject to mitigations such as human review of identified matches, is a circumstance weighing in favour of the need to provide individuals notice about the use of FRT – *Bunnings* [194].

[56] APP Guidelines [5.8]-[5.33].

[57] APP Guidelines [5.8].

[58] *Bunnings* [188], [209].

about each matter is available and direct individuals to inquire with staff or request a factsheet the entity has developed about its FRT use.

Timing of notification

Individuals should be notified about the collection of their personal information at or before the time of collection, or if that is not practicable, as soon as practicable afterwards.[59]

In considering what steps are reasonable to notify individuals about use of FRT in a timely way, entities should take into account the characteristics of the specific physical space where FRT is deployed. This could include for example whether and how individuals could be notified prior to entering the premises, or before moving into a particular part of the premises where FRT is in use. In some commercial and retail settings entities may be able to notify some or all individuals about FRT collection practices prior to their physical attendance at the premises, for example where customers are required to make an advance booking, or obtain a membership, prior to entrance or arrival.

In addition to giving individuals the opportunity to make informed choices about their personal information, advance notice of an FRT system's operation can act as an effective deterrent for persons who may be considering criminal behaviour. In this way, effective notice can both prevent and mitigate threatening or criminal conduct that an FRT system might seek to address.

Entities should consider

- What steps will you take to notify or ensure individuals are aware of each of the matters in APP 5.2 in relation to your collection of their personal and sensitive information?
- Have you ensured that individuals are specifically aware you are collecting their sensitive information for processing in an FRT system?
- If it is not reasonable to notify individuals of particular matters using signage, what other steps can you take to ensure they can be informed about your collection of their sensitive information?
- How will you ensure individuals are notified at or before the time when you collect their sensitive information?

[59] APP 5.1

Part D: Accuracy, bias and discrimination (APP 10)

Accuracy

APP entities have an obligation to take reasonable steps to ensure the personal information collected, used and disclosed is accurate, up-to-date, complete and relevant.[60]

The reasonable steps that an entity must take will depend on the circumstances including:

- The sensitivity of the personal information
- The nature of the entity holding the personal information, and
- Possible adverse consequences for an individual if the quality of personal information is not ensured. More rigorous steps are required where the information collected, used or disclosed is 'sensitive information', such as biometric data used in FRT.

Reasonable steps to ensure accuracy

APP entities should consider the reasonable steps they will need to take to ensure accuracy. These will depend on the circumstances but may require the entity to:

- Take steps to ensure the referenced database is made up of accurate and up-to-date information
- Run a trial and conduct regular testing of accuracy
- Undertake due diligence in relation to data quality practices, and
- Clearly communicate any limitations in relation to the accuracy of the FRT system.

Consider how the risk of negative outcomes arising from possible inaccuracy or error can be mitigated, for example by requiring human verification of positive matches.

FRT carries inherent accuracy risks. Entities must develop processes to check the proportion of predictions the FRT system gets right. If an FRT system is not sufficiently accurate, it may lead to:

- False negatives – a failure to identify an individual whose face is part of the reference database, or
- False positives – the matching of faces that belong to two different individuals.

Bias and discrimination

Another risk in using an FRT system is in-built bias and discrimination of certain demographic groups which may lead to adverse impacts and unfair outcomes. Even if an FRT system is highly accurate, the training data may reflect past bias and discrimination depending on the data used. Entities must ensure this is accounted for if they are using or designing an FRT system.

Entities relying on a third-party hosted FRT system must conduct their own due diligence to manage risks associated with inaccuracy, bias and discrimination. For example, entities should ensure that a third-party hosted FRT system has been subject to robust testing and monitored for evidence of

[60] APP 10.1.

inaccuracy, bias and discrimination. Further matters to consider when engaging a third-party to provide or operate an FRT system are set out below.

Entities should consider

- Do you have appropriate and robust steps in place to check the FRT system is producing accurate results?
- What strategies have been developed to manage and mitigate risks associated with false negatives and false positives?
- What due diligence have you undertaken to assess the accuracy of the FRT? For example, if you are relying on a third-party FRT system, have you been informed about the technical effectiveness and statistical accuracy?
- Have you implemented measures to mitigate risks of bias, discrimination and unfair treatment of different demographic groups prior to using an FRT system?

Part E: Data deletion and security (APP 11)

APP entities have a responsibility to take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.[61] Reasonable steps depend on the circumstances. For entities using FRT systems, circumstances include the advanced nature of FRT technology, and the fact it requires collection of large volumes of sensitive information.

Entities should consider whether information collected by use of FRT could be vulnerable to misuse or a cyber attack. This includes:

- The length of time information is stored and thus might be vulnerable to misuse
- The steps a threat actor would need to take to compromise the FRT system and gain access to sensitive information it holds
- Who will have access to the FRT system and information it contains, including biometric information and templates of scanned individuals, and of those in the database of positive matches

APP 11 further requires entities that hold personal information to take reasonable steps to delete or de-identify that information once it is no longer needed for any purpose for which it may be used or disclosed.[62] Entities should consider the length of time collected information is held in an FRT system, and whether collected information is effectively destroyed once no longer needed for the system to achieve its purpose.

[61] APP 11.1.

[62] APP 11.2.

In general, where an individual is not a match, their biometric information and template should be deleted immediately. Where individuals generate a positive match, entities should have a process to identify the period of time for which it may require the collected sensitive information in order to achieve the purpose of the collection. Entities should also consider whether there are more privacy-protective ways to achieve that purpose without retaining the sensitive information. For example, where an FRT system is used for security purposes, an entity could consider whether it is necessary to retain collected biometric information and biometric templates themselves, or if it would be sufficient to instead only retain CCTV footage of an incident, and a record that a match was made by the FRT system.

Practical considerations – security and vendor controls

The OAIC provides the following best practice considerations in relation to security:

- Secure and transient processing by design – Collection flows should be designed so that raw inputs are processed transiently and then destroyed, so that it is not possible to be used or compromised later. On-device processing is recommended to maximise security and limit sharing.
- Ring-fenced architecture – retain facial recognition data securely in a separate store with its own keys, roles and access controls.
- Retention automation – Attach specific time-to-live (TTL) to specified data and purposes and schedule deletion jobs so that they occur automatically.
- Vendor controls – Ensure that FRT vendors are contractually bound by appropriate security and retention provisions. Verify security posture through attestations, audits and other kinds of tests, as necessary.
- General technical and organisational measures – Implement strong technical and organisational security measures that surround and support the FRT system. See the OAIC's 'Guide to securing personal information' and 'Chapter 11: APP 11 Security of personal information' for more detailed guidance.

Additional resources

OAIC resources

- Australian Privacy Principles Guidelines
- Guide to undertaking privacy impact assessments
- PIA e-Learning course
- Guide to securing personal information
- Data breach preparation and response guide
- Biometric scanning | OAIC

International resources

- Global Privacy Assembly Resolution on Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology