

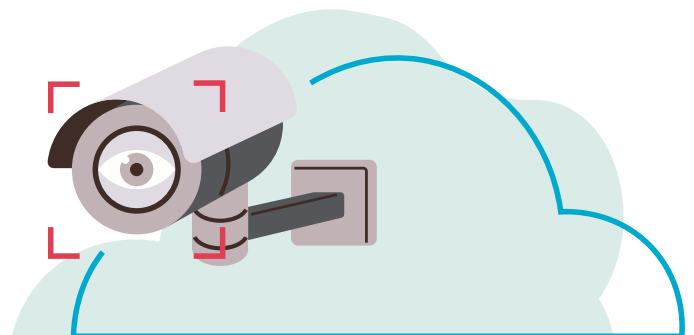


Facial recognition technology and privacy

Facial recognition technology (FRT) for identification involves collecting a digital image of an individual's face and extracting their distinct features into a biometric template, which is compared against templates in a database to identify the individual. Biometric templates are sensitive information under the Privacy Act and are afforded higher levels of protection.

Privacy need to know

- Biometric templates and photos of individuals used for the purpose of automated identification are sensitive information under the Privacy Act. Sensitive information generally has a higher level of privacy protection than other personal information. Entities must handle sensitive information with increased caution.
- A facial recognition system collects sensitive information about every person whose face it scans, not just the individuals that are a 'match', and even if that information is only held in the system momentarily. The Privacy Act applies to these collections.
- Sensitive information must be collected by consent, or on the basis of a specific exception pathway. These exceptions include when required by law, and where particular exceptional circumstances exist in relation to safety and unlawful conduct.
- In considering if an exception applies to collection of that sensitive information in a Permitted General Situation relating to serious threats or unlawful activity, entities should consider suitability, alternatives, and proportionality of their collection compared to the intrusion of privacy involved.
- Entities considering using facial recognition technology should undertake a detailed assessment of the privacy risks involved. Conducting a privacy impact assessment at the outset will help to identify and address any impacts on an individual's privacy. This will assist entities to embed good privacy practices from the start.



Key privacy considerations

Necessity and proportionality

Facial recognition technology must only be used when it is necessary and proportionate. Entities should consider whether there is a particular reason there are no alternatives, such as a unique security environment or threat profile, and carefully consider whether the benefits clearly outweigh risks posed to individuals' privacy. In jurisdictions where Workplace Protection Orders exist, the entity should consider these as an alternative to collecting sensitive information.

See Part B of the guidance

Transparency

Entities need to manage personal information in an open and transparent way. This requires entities to proactively ensure individuals are aware of a range of matters including that their information will be collected for processing by facial recognition technology, the purpose of this collection, and how the information will be handled. This includes ensuring that up to date and appropriate privacy policies and collection notices are in place.

See Parts A and C of the guidance

Accuracy, bias and discrimination

Entities need to ensure information used in facial recognition technology is accurate and take steps to address any risk of error or bias.

See Part D of the guidance

Security and data deletion

Entities must take reasonable steps to protect personal and sensitive information they collect from misuse, interference and loss, as well as unauthorised access, modification and disclosure. Entities should delete or de-identify information collected by use of facial recognition technology as soon as it is no longer needed to achieve the purpose for which it was collected.

See Part E of the guidance

Governance and ongoing assurance

Entities need to have clear governance arrangements in place, including documented practices and procedures, to minimise privacy risks. These should be implemented in practice, clearly communicated and reviewed regularly.

Where an FRT system is being operated by a third party on an entity's behalf, ensure appropriate contractual obligations are in place to ensure compliance with the Privacy Act.

See Part A of the guidance



Additional resources

Read more at [Facial recognition technology: a guide to assessing the privacy risks](#) and download the checklist and APP 3 flowchart resources