Police use of Facial Recognition Technology (FRT)

Table of Contents

Policy statement and principles

What

Facial recognition identifies or confirms an individual's identity using their face. It operates by analysing facial features and comparing them to stored images (or datasets that describe an image). FRT is a collective term for technologies and techniques involving processing of a person's facial image using statistical analysis algorithms. An algorithm compares the features of a collected image (probe) with an already stored image (source). Police is only permitted to use FRT in tightly controlled circumstances. While Police must continue to keep pace with changing technology, its use of FRT will always be lawful, ethical, proportionate, and safe.

Why

Police employees visually observing facial images in photos/videos to determine potential identity matches is a long-established policing practice. FRT is a rapidly developing technology, and its use can assist Police to deliver high quality, victim-focused services, by improving the accuracy, scale, effectiveness, and consistency of matching facial images to identities. FRT can also support operational efficiency and security, including through the Face Verification system used with Police-issued mobile phones.

Use of FRT impacts individual and collective privacy interests. A person's face is unique to that person and the biometric template which a FRT system processes is personal information, and as such is covered by the Privacy Act. In addition, unlike fingerprints and DNA, which can be used for identification in criminal proceedings, faces can change significantly over time and FRT cannot be used in isolation of best practice investigative processes.

This policy ensures that appropriate safeguards are in place for Police's use of FRT and the storage of personal information, and that use of FRT is lawful, proportionate, and appropriate in a New Zealand policing context.

How

Police will only use FRT for lawful policing functions on lawfully obtained images and data, and only where:

- use of FRT is also proportionate, having regard to human rights and privacy interests,
- use of FRT is approved, controlled, monitored, and governed,
- an audit log of the use of FRT is kept, where possible,
- standard operating procedures are in place,
- the probe image(s) is lawfully obtained,
- the source image(s) has been lawfully obtained or Police have lawful access to it,
- the analysis is required as part of an active investigation or other lawful basis,
- the FRT system has sufficiently high accuracy and does not operate with an unacceptable level of bias or discrimination,
- users of FRT have been trained in use of the tools and understand their limitations,
- Police policy and legal requirements surrounding retention, storage, and destruction of the image(s) and data are complied with,
- use of FRT is also informed by relevant guidelines and standards.

When

Appropriately trained and authorised Police employees are able to undertake retrospective facial recognition after an event for lawful policing purposes in accordance with this policy. Retrospective use is when there is a significant delay between image capture and FR processing (as defined under the EU AI Act). If there is no significant delay, then the system should be considered as operating in real-time or "live".

Although it has been demonstrated in some other jurisdictions that live FRT can be useful in certain policing scenarios, in the New Zealand context it is considered that the overall risks of live FRT outweigh the potential benefits. It follows that Police will not make decisions regarding the implementation of live FRT until the impacts from security, privacy, legal, and ethical perspectives are fully understood, and it has engaged with communities and understood their views.

Any proposals to trial or adopt live FRT must adhere to the Police chapter on Trial or adoption of new policing technology. However, in rare and extreme circumstances where there is an immediate risk to life, one-off uses of live FRT may be authorised at Superintendent-level or above if it is considered that it could be used in a safe manner to immediately minimise harm.

Definitions

Term	Definition
Biometric	A biometric is a measurement or physical characteristic that may be used to identify an individual. Biometric information is personal information, so the Privacy Act applies.
Face Detection	A subset of object detection technologies, which are designed to locate and identify various objects within an image or video. Face detection algorithms are engineered to determine the presence of human faces, but they do not possess the capability to identify specific individuals.
Face Matching	Enables the comparison of a person's face from a video or image to a reference image. This capability is useful for tracking the appearances of a person of interest across a video sequence or identifying their presence within a set of photographs. Face Matching does not identify individuals; it simply indicates whether the person in question matches a known reference image.
Face Verification	A biometric method commonly employed in modern smartphones, access control, and SmartGate systems, where the system verifies the user's identity by ensuring a match between the live capture and the reference image. It does not have the capability to identify unknown individuals.
Probe Image	A facial image that is searched against a database of images in a facial recognition system.
Source Image / Database	The image or database of images that a probe image is being matched against.

Approved examples of FRT use

The table below provides examples of situations where FRT is currently lawfully used by Police (when used in line with this policy) and the purpose for that use.

Situations where FRT is lawfully used	**Purpose**
Face Matching through automated interfaces via Forensic Services to assist in the detection of potential identity fraud or duplicate identity records when: - the first arrest photo is submitted for an offender person record in the National Intelligence Application (NIA) - creating a new firearms licensing record using a photo submitted by the applicant.	Assisting Police to detect potential fraudulent or duplicate identity records so appropriate action can be taken. This helps to maintain the integrity of identity records held by Police. Photos uploaded are transferred automatically to Police's database to be compared with existing images held by Police. Any possible matches are flagged for manual comparison and follow up action.
Face Detection and Matching for identification of an investigative or intelligence lead based on retrospective analysis of facial images from videos or photos via Forensic Services: - suspect image - victim image - missing person image - person of interest image.	Enables Police to search and compare lawfully obtained facial images from a variety of sources (including but not limited to CCTV images and digital photographs) against known identity images held by Police for lawful purposes.
Analysing/processing large quantities of videos/photos for intelligence purposes or investigations via the High Tech Crime Group	Use of technology accelerates investigations, reduces the load on staff, and speeds up victim identification. For example, automating the process to pick out content relevant to specific cases is critical in enabling Police to identify and save child exploitation victims. Use of facial recognition within these toolsets can reduce hundreds of hours of footage to selected clips of interest that Police staff can then review.
Forensic analysis on deceased persons via Forensic Services	Police Forensic Facial Examiners are trained to compare facial images using a rigorous morphological comparison and evaluation process.
Face Verification for access to Police-issued mobile phones (known as FaceID)	Enables Police staff to authenticate access securely and swiftly to their work phones.

There may also be some covert situations where the use of FRT cannot be disclosed without prejudicing the maintenance of the law, including the prevention, investigation, and detection of offences. These uses must still comply with this Policy.

Use of third-party systems and data

Police have access to some external camera systems (i.e., CCTV footage) as part of a live network with continuous access, or through data being provided retrospectively from third parties in response to specific incidents. Some of these third parties may have live FRT capabilities within their systems, which are not controlled by Police. Police does not use the live FRT capabilities of third-party systems.

Other government agencies and international partner law enforcement agencies hold facial image databases. Copies of image databases from other agencies are not held by New Zealand Police. Police may only access and share images and identity information from other agencies with legal authority and under appropriate information sharing arrangements or with court authority.

Retention, Storage and Destruction

All images held in Police FRT systems must be lawfully obtained, and retained and destroyed in line with both the Privacy Act 2020 and Policing Act 2008 (ss. 34 and 34A), as well as:

- the NZ Police Retention and Disposal Schedule - Part 1 Offence and Incident Records
- the NZ Police Retention and Disposal Schedule - Part 2 Non-Offence Records
- the Fingerprints/Biometrics policy subsection on Storage and Destruction of Fingerprints.

Tables summarising the legal basis for collection and retention of facial images are available on Ten One. Users must also be aware of the importance of image quality (including environmental conditions such as lighting and weather) for the performance and accuracy of facial recognition technology.

Governance, audit and rolling review

Governance

Primary oversight and governance of this policy is the responsibility of Police's Camera Technologies Assurance Committee (CTAC). The Executive sponsor of FRT use by Police is the Assistant Commissioner Investigations.

All FRT tools in use by Police will have an identified business owner at the Inspector-level or higher, typically the Manager of the business unit using the tool. The role of each tool's business owner is to:

- ensure the operation of the FRT tool is lawful and ethical, and continues to have appropriate human oversight,
- monitor usage and effectiveness of the FRT tool,
- ensure periodic audits are conducted to check compliance with applicable laws, regulations, standards, and policy,
- ensure that any stored facial images and biometric templates are purged from databases at the end of the agreed retention period,
- ensure and document that all personnel with authorised access to FRT are appropriately trained prior to using the system(s),
- ensure operational policy remains applicable and current and to amend accordingly,
- appropriately resolve any disputes, ambiguities or operational policy issues that need clarification, and
- ensure that any proposed trial or implementation of live FRT technology is considered in accordance with the parallel policy on Trial or adoption of new policing technology.

Audit

An audit log should exist for any FRT system to ensure that requests and searches are recorded and reviewable if necessary, however it is recognised that some of the more basic systems offering FRT capability may not provide this functionality, in which case appropriate records about access and use to these systems must be kept.

Statistics on the use of FRT must be reported to CTAC on an annual basis by each business unit using the technology.

Review

This chapter must be formally reviewed at least once every 12 months.

Additional information

Related information

See these chapters in the Police Manual and SOPs held by business groups:

- Crime Prevention Cameras (CCTV) in Public Places
- Identification of offenders
- Photography (forensic imaging), in particular the subsections on Prisoners' Photographs and Using digital CCTV evidence in law enforcement
- Maintaining the IMS Photo manager database images
- Biometrics: Fingerprints and Image Management Unit (IMU) Missing persons
- Youth justice
- Digital PhotoManager & Facial Recognition User Guide.pdf (police.govt.nz)
- Trial or adoption of new policing technology
- Identity Information Sharing.

External standards and guidelines

- NZ Algorithm Charter
- NZ Principles for the Safe and Effective Use of Data and Analytics
- OPC Guidance on AI and the Information Privacy Principles September 2023
- Data Protection and Use Policy (DPUP) | NZ Digital government
- Facial Identification Scientific Working Group (FISWG) Guidelines
- A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations (Revised 2022) | World Economic Forum, Interpol, UNICRI.