Peel Regional Police Directive

	Directive Type General Procedure	Issue Number I-B-174 (F)
Distribution All Members	Subject Use of the Facial Recognition System	
Replaces	Effective Date 2024/05/08	Next Scheduled Re-evaluation May 2025
	Last Re-evaluation Date	Re-evaluation Frequency Annual
Applicable Standards		
Special Instructions: New directive; please read entire document.		Originator Forensic Identification Services

For alternate format options, please contact Quality Assurance.

The Peel Regional Police is an organization that believes in equity, diversity and inclusion. For gender inclusivity, the pronouns "they" and "their" will be used to signify singular and plural pronouns.

Please click here to access the Religious and Cultural Guidebook. This publication should be used as a resource only, and should not be viewed as a definitive response to every situation. It is designed as an information tool that may assist our officers during investigations where religious or cultural beliefs might play a role, or impact the situation in some capacity.

Table of Contents

A. Purpose

1. The purpose of this directive is to provide all members with instructions when using or submitting a request for the use of the Peel Regional Police (P.R.P.) Facial Recognition (F.R.) System.

Back to Table of Contents

B. Policy

1. It is the policy of this Service to:

   (a) provide members with:

      (i) specific instructions and training necessary for the use of any systems and software that shall aid in the execution of their duties; and,

      (ii) clear direction regarding any specific constraints related to the performance of their duties; and,

   (b) create efficiencies in the identification of unknown individuals in a criminal investigation.

Back to Table of Contents

C. Definitions

1. For the purposes of this directive the following definitions shall apply:

   (a) "A.C.E.-V" - is the acronym for Analysis Comparison Evaluation Verification. A.C.E.-V is a scientific method utilized in most comparative processes. Verification is the final step in the A.C.E.-V method and involves the review and independent analysis of the conclusion by a qualified member of the Forensic Identification Services (F.I.S.) tasked with conducting the final examination;

   (b) "Biometrics" – refers to the measurement and analysis of unique physical or behavioral characteristics, especially as a means of determining or verifying personal identity;

   (c) "Biometric match" – means the FR software-based determination that two facial templates may have been derived from the same source based on some level of computer-evaluated similarity. The existence of a Biometric Match does not inherently imply that the person associated with the probe image and the person associated with the 'matched' image within the booking image database are the same;

   (d) "Board Agreement" – refers to the Memorandum of Understanding (M.O.U.) between the York Regional Police Services Board and the Peel Regional Police Services Board regarding the acquisition and use of the F.R. System;

   (e) "Booking Image Data" – refers to the photographic images and associated metadata (including the name of the individual, the individual's date of birth, the associated York Regional Police (Y.R.P.) or P.R.P. number, excluding C.P.I.C. data), which is collected by Y.R.P. or P.R.P. under the authority of the Identification of Criminals Act and shared by the collecting Service with the other police service in compliance with sections 32(f) and 28(2) of the Municipal Freedom of Information and Protection of Privacy Act (M.F.I.P.P.A.) via

uploaded into the F.R. Combined Data Pool by the collecting service and shared under M.F.I.P.P.A.;

(f) "Confidential Information" – refers to all Booking Image Data, Probe Images and any other confidential information or materials of a party, or of third parties and in the possession or control of Y.R.P. or P.R.P. and any information derived from any of the foregoing. Confidential information includes personal information about an identifiable individual within meaning of the M.F.I.P.P.A.;

(g) "Criminal Investigation (or Investigation)" – refers to a criminal investigation commenced by York Regional Police and Peel Regional Police that leads to or could lead to charges being laid under the Criminal Code or another Act of Parliament that provides for criminal offences;

(h) "Digital or electronic evidence" - refers to information as defined in P.R.P. Directive I-B-421 (F) "Technical Crime Services – Cyber Support Services";

(i) "Disclosure" – refers to the definition outlined in P.R.P. Directive I-B-421 (F) "Technical Crime Services – Cyber Support Services";

(j) "Entity" - refers to an individual whose identity is known or unknown and is designated by the Officer in Charge (O.I.C.) in a criminal investigation as a suspect, person of interest, victim or witness in an open and active criminal investigation;

(k) "Facial examination or (F.E.)" - refers to a human analyst undertaking a formal systematic examination (i.e. A.C.E.-V) of facial images to determine if the same person is depicted;

(l) "Facial Template" or "Template" – refers to a set of biometric measurement data prepared by an F.R. system from a facial image;

(m) "F.R. Analyst" - refers to a member of this Service who possesses the required knowledge, skills, and training necessary to operate the F.R. System. F.R. Analysts engage in the A.C.E.-V methodology to establish potential candidates for the O.I.C. of an investigation;

(n) "F.R. Combined Data Pool" - refers to the collective pool of photographic images and associated data (the Booking Image Data) uploaded into the F.R. System where it is accessible by designated F.R. Analysts from both Y.R.P. and P.R.P.;

(o) "F.R. Comparison" – refers to the automated comparison of a facial image (Probe Image) against the F.R. Combined Data Pool or Probe Image Data Pool resulting in a list of candidates ranked by computer-evaluated similarity score, commonly referred to as a one-to many comparison;

(p) "Facial Recognition System or F.R. System" - refers to the Facial Recognition cloud software licensed by the Parties, together with the Booking Image Data collected individually by each of Y.R.P. and P.R.P., and shared between the two Services in accordance with the M.O.U. and the M.F.I.P.P.A. as applicable;

(q) "F.R. System Coordinator" - refers to the Detective Sergeant assigned by the Inspector, F.I.S. to oversee the F.R. program and use of the F.R. System;

(r) “Partner Agency” - refers to a police service authorized by the signed Board Agreement to contribute to and use the F.R. System;

(s) “Person of Interest” - refers to a person whose background, relationship to the victim/complainant or the opportunity to commit the offence(s) under investigation warrants further investigation, but insufficient evidence currently exists to suggest culpability in the commission of the offence;

(t) “Potential Candidate(s)” – refers to the list of name(s) of individual(s) derived from the Biometric Matches generated by the F.R. System after the Biometric Matches have been evaluated and then screened by the F.R. Analyst to establish the Result Set;

(u) “Privacy Impact Assessment” – refers to a risk management tool used to identify the actual or potential impacts that a proposed or existing information system, technology, program, process or other activity may have on an individual’s privacy. For example, the impact of institutional privacy breaches and the consequences of the failure to comply with M.F.I.P.P.A.;

(v) “Probe Image” - refers to a facial image and/or template of an entity in an open and active criminal investigation collected in a lawful manner consistent with the Canadian Charter of Rights and Freedoms (the Charter), M.F.I.P.P.A., the common law and any applicable service procedures;

(w) “Probe Image Data Pool” – refers to the collective pool of probe images that are uploaded into the F.R. System by authorized members of this Service and exist in the F.R. System at any point in time. The Probe Image Data Pool contains probe images that have gone through an F.R. comparison, but have **not** resulted in any potential candidate matches and have **not** been removed from the system for the reasons outlined in section F.4. of this directive;

(x) “Real-Time Analysis” – refers to the live streaming of images or video for the purpose of identifying persons within the image or video;

(y) “Request for Search” - refers to the request submitted by the O.I.C. of an investigation via email to the F.R. Analyst at [redacted] with the PRP #884 , “Facial Recognition Request” attached;

(z) “Result Set” – refers to the list of potential candidates returned from a comparison conducted by the F.R. System;

(aa) “Steering Committee” – refers to a group of Y.R.P. and P.R.P. members consisting of, at minimum: the Inspector, Investigative Support Bureau (I.S.B.), the Inspector, F.I.S., and the Coordinator, F.R. System of each Service. The Steering Committee shall discuss and make decisions about issues concerning operational matters, procedures and the scope of the F.R. System. The Steering Committee shall also address any disagreements that may arise relating to the meaning or impact of the Board Agreement. The Co-Chairs of the Committee are the Senior Commanders of the F.I.S Units from each Service. The Steering Committee shall consult with Information Technology Services, I.T.S. Infrastructure and Data Centre Ops, and Legal Services as may be required;

(bb) "suspect"- refers to a person whom investigators have evidence against and believe have culpability in the commission of the criminal offence(s) under investigation;

(cc) "Y.R.P" – is the acronym for York Regional Police; and,

(dd) "witness" – refers to the definition outlined in P.R.P. Directive I-B-141 (F) "Witness Assistance and Relocation Program (W.A.R.P.)".

Back to Table of Contents

D. General

1. The Facial Recognition (F.R.) System is an investigative tool that:

   (a) assists Officers in identifying individuals during an open and active criminal investigation into offences under the Criminal Code or another Act of Parliament, the specifics of which are outlined under section G. of this directive;

   (b) aims to identify or authenticate individuals by comparing their facial geometry and generating a morphological map to compare against a database of known faces for a possible match;

   (c) requires a digital image of an unidentified individual's face of a sufficiently high quality, a database of digital images of identified individuals to compare the unknown image against, and the F.R. software that will accurately compare the morphological features during any comparison initiated; and,

   (d) shall **not** be configured to interface with any other system to perform real-time analysis.

2. The Inspector, F.I.S. shall be responsible for the administration and oversight of the F.R. program at P.R.P.

3. Only qualified F.R. Analysts are permitted to use the F.R. System.

4. Members shall **not** utilize the F.R. System or associated data for their own personal use or for any other unauthorized use.

5. Generated comparison results created with the assistance of the F.R. System are to identify a potential candidate(s), the results are **not** an exact means of identification.

Back to Table of Contents

E. Booking Image

1. Booking Image Data consists of photographic images and associated metadata including name, date of birth and designated police identification number collected by York Regional Police or Peel Regional Police under the authority of the Identification of Criminals Act, R.S.C., 1985, c. I-1.

2. Booking Image Data is uploaded into the F.R. Combined Data Pool by the service responsible for collecting the Booking Image and is made available to the other service for the purpose of utilizing the F.R. System.

3. Booking Image Data shall be deleted from the F.R. Combined Data Pool by the collecting police service in accordance with that service's record retention bylaw and/or destruction of Booking Image procedures (i.e. for Youth Criminal Justice Act matters, pardons, destruction requests etc.).

4. Booking Image Data shall be deleted from the F.R Combined Data Pool by the system interface ensuring all data is up to date and records deleted and sealed are automatically removed from F.R Combined Data Pool.

Back to Table of Contents

F. Probe Images

1. The Probe Image Data Pool consists of individuals who have been designated by the Lead Investigator as an Unknown Entity in an open and active criminal investigation.

2. Probe Images uploaded into the F.R. System's Probe Image Data Pool:

   (a) can only be derived from photographs and stills of video images;

   (b) shall be collected, seized or obtained by Y.R.P. or P.R.P. in a lawful manner as part of a criminal investigation;

   (c) shall form part of the digital evidence associated to the relevant investigation;

   (d) are uploaded by the Service responsible for collecting the Probe Image and the associated investigation (or, in the case of a joint investigation, the lead agency);

2. The Probe Image Data Pool is managed by the uploading Service and is made available to the other Service for the purpose of utilizing the F.R. System.

3. Probe Images of suspects or persons of interest shall be deleted from the Probe Image Data Pool by the collecting police service as follows (whichever is sooner):

   (a) as soon as a suspect or person of interest is identified with assistance of the F.R. System or otherwise;

   (b) within 30 days of when the associated criminal investigation closes;

   (c) by the date or within the timeframe specified by the Court, if the original image, information or record from which the Probe Image was taken is ordered to be disposed of by the Court and any appeals from that order have been concluded;

   (d) as may be otherwise required by applicable law;

(e) within 30 days of a final determination that the Probe Image was later deemed to be unlawfully collected;

(f) in accordance with the service's directives and procedures concerning records retention;

(g) where the Probe Image no longer forms a relevant part of the criminal investigation; or,

(h) where the Lead Investigator has determined that the person is no longer a suspect or person of interest.

4. The Facial Recognition, Analyst, F.I.S., shall delete probe images of victims or witnesses from the Probe Image Data Pool as soon as an F.R. Comparison has been conducted regardless of result.

5. The Coordinator, F.R. System shall arrange for an audit of Probe Images that have been in the Probe Image Data Pool for longer than 12 months to determine whether any of the conditions in section F.4. of this directive exist such that the Probe Image should have been deleted from the F.R. System.

Note: If images that should have been deleted are found, the F.R. Analyst shall re-evaluate the image against section F.4 for retention.

Back to Table of Contents

G. Authorized Uses

1. In general, the F.R. System may **only** be used to:

(a) assist police to efficiently and accurately investigate criminal offences by supplementing traditional investigative methods with biometric technology for the purpose of identifying unknown Entities in open and active criminal investigations; or,

(b) for the purposes and in the manner set out in a judicial authorization obtained under the Criminal Code or another Act of Parliament.

2. In the case of unknown suspects or persons of interest, Lead Investigators may submit a request to the F.R. Analyst, F.I.S. for a F.R. Comparison in the following circumstances:

(a) the criminal investigation is open and active;

(b) the Lead Investigator does **not** know the identity of a suspect or person of interest and that identity would assist in advancing the investigation; and,

(c) the Probe Image was obtained as part of the criminal investigation and is in the lawful possession of P.R.P.

3. In the case of known suspects or persons of interest, Lead Investigators may submit a request to the F.R. Analyst, F.I.S. for F.R. Comparison where it would advance the criminal investigation to confirm whether the person on the Probe Image is in the F.R. Combined Data Pool under another name.

4. In the case of unknown victims or witnesses, Lead Investigators may submit a request to the F.R. Analyst, F.I.S. for a F.R. Comparison only in the case of emergent situations where immediate action is required for public safety or police safety. These requests shall be reviewed by the Inspector, F.I.S. before the F.R. System is engaged. Victim and witness images shall **only** be compared to the F.R. Combined Data Pool and shall **not** be compared to the Probe Image Data Pool; and,

5. Members requesting the use of the F.R. System shall be aware that the generated results of potential candidates are **only** possible matches and **not** an exact identification. As such, the results are only to be treated as an investigative aid. Possible matches still require the corroboration of evidence and a thorough investigation. The results of F.R. do **not** in and of itself provide reasonable and probable grounds for arrest and/or search authority.

Back to Table of Contents

H. Unauthorized Uses

1. Subject to section B.1.(b) of this directive, the use of the F.R. System for any purpose other than the cases stated in section G. of this directive is unauthorized and **not** permitted.

2. The following example uses of the F.R. System are unauthorized:

   (a) to assist investigators identify a person who the Lead Investigator has **not** yet been deemed to be a suspect or person of interest (or a victim or witness, where the preconditions in section G.4. of this directive exist);

   (b) to compare images that are neither Probe Images or Booking Images;

   (c) to aggregate or match multiple Result Sets from the F.R. System to locate trends or for another purpose, except for purposes of statistical analysis under the M.F.I.P.P.A. and the Anti-Racism Act;

   (d) for the purpose of tracking or monitoring an individual's movements; or,

   (e) for any live stream / real time identification purposes.

3. Unauthorized uses of the F.R. System may constitute a breach of M.F.I.P.P.A., the Charter, the Human Rights Code of Ontario, or another law and/or be contrary to the M.O.U.

4. The existence of judicial authorization with respect to a specified use of the F.R. System obtained under the Criminal Code or another Act of Parliament supersedes the limitations that this directive or the Board Agreement places on use.

Back to Table of Contents

I. External Police Agencies

1. Members who received requests from an outside police agency to conduct a comparison in the F.R. System shall advise the outside agency that they must send their requests to [redacted]

2. The F.R. Analyst or F.R. Coordinator shall send the requesting agency a blank request form, P.R.P. #884 "Facial Recognition Request" along with an information package that outlines all roles, responsibilities and expectations of the requesting agency. This shall include preconditions of use consistent with this directive.

3. Probe Images received by an outside police agency shall **not** be stored in the Probe Image Data Pool and shall be deleted by the F.R. Analyst, F.I.S. as soon as the search has been completed regardless of result.

Back to Table of Contents

J. Responsibilities – Uniform Officers

1. When it is determined that a photograph or video exists of an unidentified suspect(s) related to an ongoing investigation, and a request for the suspect image to be searched on the F.R. System is required, Officers shall:

   (a) lawfully obtain a copy of the subject probe image (e.g. photograph, video or composite drawing) pertaining to the investigation. Where an Officer is uncertain of the lawfulness of the probe images, Officers shall consult with the Crown Attorney's office and/or in-house legal counsel. If a video is the media being searched, a time frame of interest shall be provided;

   (b) complete and submit P.R.P. #884, with supporting probe images via email to the intake email site at F.I.S., [redacted]; and,

   (c) record all relevant information in compliance with P.R.P. Directive I-B-134 (F) or any other directives dealing with "Sworn and Designated Members Notebooks".

2. If the use of the F.R. System is deemed urgent or an emergency, Officers shall:

   (a) submit a request to their immediate Supervisor who shall record the reasons for requesting an emergency use;

   (b) where it is **not** immediately possible for the immediate Supervisor to provide their decision in writing, their authorization may be given verbally;

   (c) record verbal authorization in writing as soon as is practicable and forward to the Inspector, F.I.S. advising of the time, date, and reasons for use; and,

   (d) email all relevant information to [redacted]

3. Upon receipt of the search result set (candidate list) information, Officers performing a criminal investigation shall:

   (a) perform a background investigation for all the possible leads in the report;

   (b) review investigative actions on the Investigative Lead Report with their Supervisor;

(c) update Niche with all pertinent information and ensure an email is sent back to [redacted] indicating the results of the information that was provided; and,

(d) where the Officer receives a response to a search request, **not** use the image provided for any other purpose other than for which the request was made.

4. The O.I.C. of an investigation shall:

(a) complete the Responsibilities and Ethical Use of Facial Recognition Training available in the Canadian Police Knowledge Network (C.P.K.N) site;

(b) determine whether the desired purpose in using the F.R. System is for an authorized use as described in this Directive;

(c) complete and submit the F.R.S. Request Form, P.R.P. #884;

(d) record all relevant information in their notebook;

(e) ensure the name of the potential candidate(s) is checked for validity on C.P.I.C.;

(f) perform background investigation(s) for all result set possible candidate(s) in the report (e.g. canvass, castoffs, interviews, photo line-ups, background checks, cell dumps, etc.);

(g) notify the F.R. Coordinator should any circumstances arise to remove a probe image from the F.R. System; and,

(h) understand that results are **not** a positive means of identification and are only an investigative aid, which required corroboration of evidence by way of a thorough investigation.

Back to Table of Contents

K. Responsibilities – Facial Recognition Analyst, Forensic Identification Services

1. The Facial Recognition Analyst, F.I.S. shall:

(a) review information provided to ensure compliance with this procedure and that sufficient information has been provided to decide whether a proposed use is authorized under section G. of this directive;

(b) decline to conduct the F.R. search or comparison where the preconditions are **not** met for an authorized use, images are of an insufficient quality **not** suitable for comparison, or insufficient information was provided;

(c) conduct F.R. search and comparisons; and,

(d) remove probe images of suspects or persons of interest from the Probe Image Data Pool.

2. Upon receipt of P.R.P. #884, the Facial Recognition Analyst, F.I.S. shall:

(a) review the details of all information provided ensuring compliance with F.I.S. specific policies on the purpose of the search request;

(b) initiate the request in Niche for tracking purposes;

(c) create an investigation in the F.R. System with the Occurrence number in the request;

(d) perform analysis on probes submitted (e.g. enhancements, observations, notes);

(e) conduct a search of probe images against existing mugshots of known offenders;

(f) analyze results for any possible candidates, have another Analyst perform a peer review and take note who performed the review as part of the process;

(g) generate an email to the requester with the subject, “Investigative Lead Report” or “No Match Report”; and,

(h) assign a task in Niche for the Officer to review the Report.

Back to Table of Contents

L. Responsibilities – F.R. System Coordinator, Detective Sergeant, F.I.S.

1. The Facial Recognition System Coordinator, Detective Sergeant, F.I.S. shall:

(a) be responsible for the storage, retention, and disposal of booking image data;

(b) ensure the upload of booking image data into the F.R. Combined Data Pool which will be made available to Y.R.P. as booking image data collected by Y.R.P. will be available to P.R.P. for the purpose of utilizing the F.R. System in accordance with this directive and the established M.O.U.;

(c) ensure the removal of booking image data from the F.R. Combined Data Pool in accordance with P.R.P. Directive I-A-607 (O), or any other directives dealing with “Records Retention, Storage and Disposition”;

(d) arrange with I.T.S. to conduct an audit of probe images that have been in the probe image data pool for longer than 12 months to determine whether any of the conditions in section F.4. of this directive exist such that the probe image should have been removed from the F.R. System; and,

(e) ensure all F.R. requests meet with and comply with the directive requirements set out in section G. of this directive.

Back to Table of Contents

M. Responsibilities – Inspector, Forensic Identification Services (F.I.S.)

1. The Inspector, F.I.S. or designate shall:

(a) ensure all F.R. requests are completed in a timely manner;

(b) create a monthly report on all emergency uses for the F.R. System;

(c) conduct regularly scheduled audits to ensure that system permissions are appropriate, the F.R. System is deployed as designed and qualified operators are in compliance with this directive;

(d) attend Steering Committee meetings as Co-Chair;

(e) ensure complete and accurate records are maintained for all requests made and searches conducted;

(f) ensure all F.R. requests are maintained and carried out by qualified F.R. Analysts; and,

(g) liaise with Legal Services for any requests and use of facial recognition in exigent circumstances outside the authorized uses of the F.R. System.

Back to Table of Contents

N. Responsibilities – Director, Information Technology Services (I.T.S.)

1. The Director, I.T.S. shall:

(a) provide support to Officers and F.R. System Operators when requested;

(b) work with F.R. System vendor to resolve any technical issues and ensure the System is properly maintained; and,

(c) provide system, operational, and audit reports to the Inspector, F.I.S.

Back to Table of Contents

By Order Of:

N. Duraiappah
Chief of Police