# Client Advisory: Overview of The IPC's Guidance on Facial Recognition and Mugshot Databases Used By Ontario Police Services

Elisabeth Symons, Olalekan (Wole) Akinremi, M. Imtiaz Karamat, and Victoria Di Felice March 20, 2024

## Introduction

Facial recognition (FR) technology, a form of artificial intelligence (AI) technology that collects and processes sensitive personal information to identify or verify an individual's identity, has the potential to significantly improve the speed and scale of police-operated mugshot databases. However, the use of FR technology by law enforcement raises legal, privacy, and ethical questions that are not fully resolved by Canada's current laws relating to the identification of criminals[1].

To date, there are a few guidance documents that draw attention to these issues, providing analyses of the issues and advancing thoughts on best practices. These guidance documents include: (i) the joint statement on the *Recommended legal framework for police agencies' use of facial recognition* issued by the Federal Provincial, and Territorial Privacy Commissioners;[2] and (ii) the *joint statement by the Information and Privacy Commissioner of Ontario and the Ontario Human Rights Commission on the use of AI technologies*.[3]

Recently, the Information and Privacy Commissioner of Ontario (IPC) issued its guidance document titled *Facial Recognition and Mugshot Databases: Guidance for Police in Ontario* (the Guidance).[4]

The Guidance is non-binding, and through it, the IPC seeks to clarify the privacy obligations of Ontario police services that already use or are planning to use FR technology in connection with mugshot databases. The Guidance offers recommendations for the responsible use by the police of FR technology in connection with mugshot databases, and it adds to the discussion of the related legal, privacy and ethical questions.

This Advisory provides an overview of the IPC's Guidance and is organized as follows:

(i) a summary of the IPC's key considerations and recommendations, which is divided into: (A) Pre-Implementation Stage Recommendations, (B) Operational Stage Recommendations, and (C) Program Review Stage Recommendations; and

(ii) a checklist to assist those who need to action the IPC's recommendations for implementing a FR mugshot database program.

***This Advisory is not intended to be a statement of the law and does not constitute legal advice. As this Advisory is for information purposes only, no person should act or rely upon the information contained in this Advisory without seeking legal advice.***

---

[1] The laws relating to the identification of criminals and the rights of individuals who may be affected by law enforcement's practices relating to the identification of criminals include: (i) the Identification of Criminals Act (R.S.C., 1985, c. I-1) (ICA), (ii) cases relating to the ICA; (iii) the Canadian Charter of Rights and Freedoms (the Charter); (iv) the federal, provincial and territorial human rights acts; and (v) the applicable federal, provincial and territorial privacy acts.

[2] The Office of the Privacy Commissioner of Canada, "Recommended legal framework for police agencies' use of facial recognition" (2 May 2022), online: priv.gc.ca < https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2022/s-d_prov_20220502/>.

[3] Information and Privacy Commissioner of Ontario, "Joint statement by the Information and Privacy Commissioner of Ontario and the Ontario Human Rights Commission on the use of AI technologies" (25 May 2023), online: ipc.on.ca < https://www.ipc.on.ca/newsrelease/joint-statement-by-the-information-and-privacy-commissioner-of-ontario-and-the-ontario-human-rights-commission-on-the-use-of-ai-technologies/>.

[4] Information and Privacy Commissioner of Ontario, "Facial Recognition and Mugshot Databases: Guidance for Police in Ontario" (Jan 19, 2024), online: <https://www.ipc.on.ca/wp-content/uploads/2024/01/2024-01-19-facial-recognition-and-mugshot-databases-guidance-for-police-in-ontario-e.pdf> [The Guidance].

## Key Considerations and Recommendations

The following summarizes the IPC's recommendations and rationale for police in Ontario to take before (Pre-Implementation Stage), during (Operational Stage), and after (Program Review Stage) implementing an FR mugshot database program. This is not an exhaustive list and, as noted in the Guidance, police may also need to implement further privacy protections depending on the nature, complexity, and scope of the risks posed by their specific program.

## A. Pre-Implementation Stage

### 1. Lawful Authority and Lawful Operation

When police infringe upon a person's reasonable expectation of privacy, the police are required to **have lawful authority and to act lawfully**. This principle and the related laws apply to the implementation and operation of any use of FR in relation to a mugshot database. FR mugshot database programs involve the collection, retention, use, and disclosure of personal information, which can impact the reasonable expectation of privacy of individuals.

***IPC's Recommendations:***

1.1. Ensure there is lawful authority to operate a FR mugshot database program before starting the program and clearly document such authority. If you are already operating a program, re-evaluate lawful authority as soon as possible.

1.2. Ensure the design and operation of the program, including any use of third-party service providers, meet all legal requirements, and include privacy and transparency safeguards and controls.

1.3. Adjust the scope of the FR mugshot database to account for any gaps and ensure compliance.

***Practices to Consider When Implementing the IPC's Recommendations***

- Conduct a review of lawful authority in relation to any proposed use(s) of FR for mugshot databases to better understand if the use is clearly lawful, likely lawful, likely unlawful, or clearly unlawful because: (i) it is easier to make adjustments to the use(s) so that they are likely lawful or clearly lawful while the program is being designed; (ii) doing so will help to make sure that the chosen tools are best suited for the proposed use(s); (iii) it means knowing the commitments that are required from the vendor(s) of those tools when there is an opportunity to negotiate and have them added to the applicable contract.
- To document lawful authority for the use of FR in relation to a mugshot database, consider setting out the authority in the documents that are used to seek approval for and otherwise implement the practice. This could include: (i) the recommendation to procure the necessary tools; (ii) the procurement documents for the necessary tools; (iii) policies relating to the use of the tools; (iv) procedures relating to the use of the tools; and (v) training materials.
- Use the procurement process to support the inclusion of provisions necessary for compliance with laws (including those relating to privacy and transparency safeguards and controls) when acquiring FR tools.

## 2. Guiding Principles

The IPC notes that both public trust and community acceptance of FR mugshot database programs will depend on the principles adopted by police to guide those programs and the efforts of the police to comply with those principles. The importance of transparency and communication to foster trust and community acceptance is stressed in the Guidance, and the Guidance includes a minimum set of principles that police in Ontario should commit to when using FR.

***IPC's Recommendations:***

2.1. Publicly communicate a statement of guiding principles for the use of the FR mugshot database that addresses the delivery of fair, effective, and equitable policing services in a manner that protects and advances privacy, transparency, accountability and human rights.

2.2 Respect and adhere to these principles throughout all stages of the development and operation of the FR mugshot database.

***The IPC's Minimum Set of Principles to Guide the Use of FR***

A statement of principles should commit to using FR in a way that is:

- is necessary and proportionate to the purposes of the program
- respects human rights and upholds human dignity as a fundamental value
- respects individuals' rights to privacy and access to information
- prevents harms to individuals and groups
- is transparent and accountable to the public
- always involves human oversight and interpretation of results by trained operators
- treats all potential matches as investigative leads only
- evaluates system performance and mitigates inaccuracy and bias as much as possible
- upholds the integrity of the criminal justice system and the administration of justice
- achieves community safety objectives that outweigh the risk of harms

## 3. Mugshot Databases and Related Policies

The Guidance refers to the increasing amount of evidence suggesting that arrest records contained within mugshot database programs may be linked with discriminatory or disproportionate policing. Consequently, the IPC advises police to consider this issue when planning their programs to use FR in relation to mugshot databases, including by **establishing appropriate retention and destruction requirements** for images included in their mugshot database to ensure that mugshot records are retained for only as long as is necessary and proportionate. Additionally, young people, racialized and Indigenous persons, individuals who have never been convicted of a serious crime along with other vulnerable individuals and communities should be protected against the excessive retention and use of their personal information in a mugshot.

***IPC's Recommendations:***

3.1. Review arrest record policies and retention schedules governing mugshot databases to ensure that they do not permit or facilitate the discriminatory, unconstitutional, or otherwise unlawful retention and use of mugshot records.

3.2. At the pre-implementation stage and on an annual basis moving forward, purge mugshot databases of records that may facilitate excessive, discriminatory, or unlawful police practices, including by purging.

3.3. For those currently operating a FR mugshot database, review and purge mugshot records in accordance with above 3.1-3.2 as soon as possible, but no later than one year following the release of the Guidance and on at least an annual basis moving forward.

***Practices to Consider When Implementing the IPC's Recommendations***

- When considering a FR tool, check if each record that includes a mugshot already has or can be configured to include the categories of information needed to maintain the database in accordance with the IPC's recommendations. For example, does each record include a flag indicating:
  - whether or not a conviction resulted from the arrest;
  - whether the charges laid were summary or indictable; and
  - whether the charges were laid under the *Youth Criminal Justice Act* (YCJA).
- When considering a FR tool, check if the tool includes functions that will make purging images from the associated mugshot database more manageable. For example:
  - can administrators use a single command to delete all records in the mugshot database that relate to charges under the YCJA that: (i) were dismissed or withdrawn; and (ii) prior to the next scheduled purge, will exceed the provided retention period; or
  - is the tool capable of automatically setting the deletion date for a record that relates to a summary conviction when the conviction is entered; or
  - is the tool capable of generating a report that identifies all records in the mugshot database that have a deletion date in a given time period?

## 4. Privacy Impact Assessments

The Guidance notes that privacy risks associated with FR mugshot database programs include the potential misuse of personal information, potential bias and inaccuracy, and technological or human errors that could result in false recognitions and wrongful arrests. The IPC advises police to **conduct a Privacy Impact Assessment (PIA)** to assist in understanding the relevant privacy risks, obligations, and mitigation measures. This process should be documented in a PIA report that addresses all privacy risks and explains the related risk mitigation strategies.

**Risk mitigation strategies** should include:

- documented policies and procedures for limiting the purposes of FR searches;
- logging all related uses and disclosures of personal information; and
- assigning senior staff with clear roles and responsibilities for monitoring privacy risks and ensuring compliance.

***IPC's Recommendations:***

4.1. Conduct a PIA and document the process in a PIA report prior to putting in place a FR mugshot database program, including before a pilot program and any time there are significant changes made to an existing program.

4.2. The PIA report should identify and address the privacy risks of using FR technology in the mugshot database context and include safeguards and controls that can be built into the program's policies and procedures to mitigate these risks.

4.3. The results of the PIA should be shared with the police services board and the PIA report, or summary of it, should be made publicly available for transparency and accountability purposes.

4.4. Conduct other risk assessments such as security, human rights, and algorithmic impact assessments as needed, and ensure these are combined or coordinated with the PIA.

***Additional Practices to Consider When Mitigating Risks Relating to Implementing a FR Mugshot Program***

- As part of the procurement process when acquiring a FR tool, assess the ability and the willingness of the applicable vendor to support the conduct of a PIA and the other type of risk assessments that the IPC recommends.
- When acquiring a FR tool, assess the extent to which the: (i) tool includes safeguards and controls that support compliance; and (ii) contract for the provision of the FR tool provided by the applicable vendor commits to maintaining those safeguards.
- Assess the extent to which safeguards can be implemented without the applicable vendor's participation.

***The IPC's Recommended Considerations for Conducting a FR Mugshot Program PIA***

Consider that FR mugshot databases:

- involve the collection of new and sensitive personal biometric information[5] that is separate from the photographs used to create that information;
- impact the privacy of all individuals whose personal information may be implicated in the operation of a FR system;
- are one part of a system of arrest records that police have been gathering for many years, including non-conviction arrest records;
- are an application of FR technology that operates without the knowledge or consent of affected individuals;
- are used to generate investigative leads, including those that may cause unwarranted scrutiny and unnecessary or disproportionate record keeping; and
- may facilitate the disclosure of personal information to police in Ontario and other law enforcement agencies in Canada or other countries.

## 5. Program Scope, Purpose and Policies

The IPC recommends that police should **define and limit the scope and purpose** of their FR mugshot database program to manage it responsibly and to remain aligned with the privacy principles of reasonableness, necessity, and proportionality. The IPC explains that a properly defined program should concentrate on creating investigative leads aimed at identifying individuals who are reasonably suspected of committing an offence.

[5] "Biometric information" is personal information that relates to the physical characteristics of an individual.

***IPC's Recommendations:***

5.1. Establish and limit the scope and purpose of the FR mugshot database program by focussing on generating investigative leads for the purpose of identifying individuals reasonably suspected of having committed a serious offence. The scope and purpose of the FR mugshot database program should be maintained over time and comply with applicable laws and the privacy principles of reasonableness, necessity, and proportionality.

5.2. Develop and approve policies and procedures for the FR mugshot database program consistent with the IPC's recommendations.

## 6. Public Engagement

The IPC recommends that police **conduct public engagement activities** with community members (including those: (i) whose personal information may be contained in the database; or (ii) who belong to communities that are disproportionately represented in mugshot databases) and subject matter experts to have a dialogue about privacy and equity concerns as they relate to the use of FR for mugshots. This consultation should address how the police will use FR and protect fundamental rights. The IPC states that publicly considering the privacy and human rights issues raised by FR before putting an FR mugshot database program into place will promote accountability and transparency.

***IPC's Recommendations:***

6.1. Conduct public consultations with affected communities and interested parties about your program. If your program is current or ongoing at the time that the Guidance is issued, then public consultations should still occur.

6.2. During public consultations, ensure privacy and equity concerns of marginalized communities, including those who are disproportionately affected by systemic discrimination and over-policing practices are considered.

***Practices to Consider When Implementing the IPC's Recommendations***

- Challenges may arise when carrying out public consultations for a FR mugshot database program that was already implemented without prior public consultation. A portion of the audience may already believe that there have been violations of their or someone else's reasonable expectation of privacy. That belief (whether incorrect or correct) will influence how they interact. When preparing for this type of exercise, it is a good idea to create a multi-disciplinary team that involves members with expertise in communications, privacy, legal, and law enforcement.

## 7. Transparency

The IPC advises police to be **transparent with the public** about the implementation and operation of their FR mugshot database program. This helps to build and maintain public trust, especially with vulnerable and over-policed communities.

***IPC's Recommendations:***

7.1. Publicly post up-to-date, readily available, plain language information about the FR mugshot database program on the websites of both the police services board and the police service to foster ongoing transparency.

***The IPC's Recommendations for What to Include in the Public Information About a FR Mugshot Database Program***

- the most current version of the program's policies and procedures
- the PIA and other risk assessments or, at a minimum, summaries of these assessments

- a plain language explanation of how the program works, including its scope and purpose, lawful authority, and safeguards and controls
- details about public consultations that have taken place, including a general description of the consultees, the nature of the consultation (focus groups, meetings, surveys), and a general summary of what was heard
- information about the procurement of the FR system, including information about third-party service providers and their compliance with privacy obligations
- results of any testing for accuracy or bias, including a general description of the testing methodology
- statistics measuring the overall effectiveness of the program

## 8. Pilot Program

The IPC recommends that police conduct a time-limited **pilot program** to identify any issues and adjust components of the program, the PIA, and any relevant policies and procedures before pursuing final implementation.

***IPC's Recommendations:***

8.1. Conduct a time-limited pilot project with clear goals and objectives before fully implementing the FR technology. Use the pilot to test the program and ensure its effectiveness in achieving the intended results, to identify and address any unintended issues or consequences, and to mitigate risks to privacy and human rights.

8.2. Evaluate and publicly report on the results of the pilot before implementation by sharing key findings with affected communities and interested parties as part of a meaningful public engagement process.

***The IPC's Recommendations for What to Evaluate When Conducting a Pilot FR Mugshot Database Program***

At a minimum, the pilot FR mugshot database program should evaluate:

- whether the intended benefits of the system are realized and if any unforeseen risks or harms have appeared
- whether FR search requests and procedures are being followed correctly, including having effective documentation
- whether staff have sufficient training to interpret matches returned by the system after a search query, and to understand the capacities and limits of the system
- whether system parameters, such as minimum threshold settings for a match, are set appropriately or need to be adjusted (e.g., to avoid false positives)
- whether there is any evidence of errors, inaccuracy, or bias in system outputs or in staff or officer interpretation of those outputs

## B. Operational Stage

### 9. Quality of Probe Images

The IPC recommends that police in Ontario **set minimum standards for the quality of probe images**[6] to: (i) support the accurate and lawful use of FR technology; (ii) reduce the risks of misidentification; and (iii) assist with FR mugshot database review and evaluation.

***The IPC's Advice on Quality of Probe Images***

Specifically, the IPC recommends the following list:

- setting standards for pixel density, lighting, percentage of face that is visible, and any other factor that is likely to significantly impact the accuracy of a FR system's search results;
- avoiding the use of artist or composite drawings or photos of lookalike individuals as probe images; and
- avoiding digitally altering probe images. If altering an image is justified, (e.g., blurring the faces of individuals in the background to protect their privacy), then ensure to document to steps taken.

***IPC's Recommendations:***

9.1. To support the lawful and accurate use of FR, set and follow clear standards for ensuring minimum photo quality of probe images consistent with the standards recommended in the Guidance.

### 10. Retention of Probe Images

The IPC advises police to set policies for how long probe images are retained. Police should ensure that their FR mugshot database program does not automatically save, store, or retain probe images. Furthermore, unless required under law, probe images should only be retained for as long as necessary. This retention period also applies to **unidentified probe images.**[7]

[6] A "probe image" is the image that is fed into the FR tool with the hope of obtaining a match.
[7] An "unidentified probe image" refers to an image that will not register a match when searched against a mugshot database.

***IPC's Recommendations:***

10.1. Set clear rules and processes for how long probe images, including unidentified probe images, should be retained and when they should be securely destroyed.

10.2. Set an appropriate oversight process for regularly confirming compliance with applicable retention and destruction rules for probe images, including unidentified probe images.

***The IPC's Advice on the Retention Period for Unidentified Probe Images***

Unless required by law, unidentified probe images should be destroyed as soon as any one of the following circumstances apply:

- the person is no longer a suspect in the associated criminal investigation;
- the unidentified probe image is no longer relevant to the associated criminal investigation;
- within 30 days of when the associated criminal investigation closes;
- within 30 days of a final decision that an unidentified probe image was unlawfully collected;
- the police services board's record retention rules require destruction; or
- destruction is required by law (e.g., by a final court order).

Further, any retention of probe images, including unidentified probe images, for testing purposes should be limited to what is necessary to meet accuracy and other performance requirements for the FR mugshot database program. Once testing is completed, the images should be immediately destroyed.

## 11. Accuracy, Human Review, and Oversight of Results

Police should document and explain how the results of FR searches will be interpreted and acted on to ensure accuracy, fairness, bias-free service delivery, and overall effectiveness of the FR mugshot database program. While emphasising the importance of human oversight, the IPC explains that the failure to carefully review search results or placing too much confidence in them could result in unnecessary or unfair investigations of individuals. Further, given that FR systems can vary in quality, reliability, and accuracy rates, the accuracy of the FR system and the results should not be assumed.

***IPC's Recommendations:***

11.1. Take steps to test for bias and inaccuracy in the performance of the FR system on a regular basis. This should include internally evaluating whether system parameters, such as minimum threshold settings for a match are set appropriately or need to be adjusted.

11.2. Set and follow transparent procedures for the human review and accuracy controls of the FR mugshot database program. These procedures should outline who is responsible for conducting the

***Practices to Consider When Implementing the IPC's Recommendations***

- When procuring a FR tool:
  - assess the applicable vendor's program for the testing of accuracy (e.g., consider the methods used, frequency of the tests, accuracy percentage that the vendor deems appropriate for its FR tool, and whether any testing has been conducted on the FR tool as it relates to communities that are disproportionately represented in mugshot databases);
  - assess the program(s) used by the applicable vendor to test for bias;
  - ask about the vendor's response when an accuracy or a bias problem is identified;

review, how trained operators interpret and explain the results of FR searches and the training requirements necessary for the job. Trained operators should follow clear criteria and be able to provide a clear explanation of the steps and processes followed for generating investigative leads.

11.3. Set and follow requirements for documenting all FR searches and assessment results. This documentation should cover the probe image and match threshold that was used, the likelihood of a match, the output as determined by the FR system, the trained operator who conducted the search, the operator's post-assessment decision on whether to treat a potential match as a false positive or a potential investigative lead, and any other relevant information.

- check the applicable vendor's standard form contract to see if its provisions support the claims being made; and
- pay attention to the reports that the FR tool can generate to support the testing of its: (i) overall accuracy; and (ii) accuracy relating to individuals who are part of disproportionality represented communities.

- Criteria for establishing when a result generated by the FR tool should become an investigative lead should be well documented, and the efficacy of the criteria should be documented and inform regular reviews of the criteria.
- Ensure that individuals who provide human oversight to a FR tool are trained to understand and account for: (i) techno-chauvinism (a belief that solutions based on technology are inherently superior to other solutions); (ii) match thresholds; (iii) accuracy rates; (iv) FR as a lead generation tool, not proof of identity; and (v) the importance of them making their own determination on whether a result from the FR tool should become an investigative lead.

## 12. Limited Collection, Retention, Use, or Disclosure of Personal Information and Reasonable Safeguards

The IPC states that police services in Ontario must collect, retain, use or disclose personal information in accordance with their obligations under FIPPA and MFIPPA. Consequently, policies and procedures should ensure that the **collection, retention, use, or disclosure of records related to the FR mugshot database program is limited and in compliance with the law**. Additionally, Police should ensure that reasonable security measures are in place to protect the personal information involved in the FR mugshot database program. This is especially the case for biometric information, which warrants special attention due to its increased sensitivity relative to other types of personal information.

***IPC's Recommendations:***

12.1. Ensure that the collection, retention, use, or disclosure of personal information is limited to what is necessary and proportionate for achieving the stated purpose of the FR mugshot database program.

12.2. Ensure that requirements for the collection, retention, use or disclosure of personal information are well documented in supporting policies and procedures and account for the distinct parts of the FR program (e.g., mugshot databases, probe images, and training data).

12.3. Adopt comprehensive administrative, technical, and physical controls and safeguards for the collection, retention, use, or disclosure of personal information involved in the program, including safeguards that protect biometric data.

## 13. Access, Correction, and Expungement Rights

***IPC's Recommendations:***

13.1. Ensure polices and procedures comply with and accommodate access, correction, and expungement rights.

13.2. Make policies and procedures and plain language information about access, correction, and expungement rights publicly available.

In accordance with applicable privacy laws, **individuals have a general right to access and correct their personal information** in the custody or control of police forces.[8] This means that the processes police have in place to respond to such access requests need to address what happens when this information is in a database associated with a FR tool.

Expungement is also a concern that should be address by implementing appropriate processes. For example, when a criminal charge results in withdrawal, dismissal or otherwise results in a non-conviction, the individual charged may request that their record of arrest (including their mugshot) be expunged.

## 14. Request From Other Police Services

There may be instances where one police service (Assisting Police Service) is asked to run a FR search with a probe image on behalf of another police service (Requesting Police Service). The Guidance suggests police have **a standard form for use by Requesting Police Services** that outlines terms and conditions to be met before the Assisting Police Service approves the request.

***IPC's Recommendations:***

14.1. Set and follow clear policies and procedures for handling FR requests from other police services, including policies and procedures for

- receiving and processing requests from requesting police services to run FR searches in the assisting police service's mugshot database;
- disclosing the results of any potential matches to the requesting police service; and
- maintaining detailed records and logs of all access and disclosures of personal information (e.g., FR search requests received).

***The IPC's Advice on the Recommended Standard Form***

The form should include the following terms and conditions:

- the request for a probe image search must be submitted in writing;
- the request is for a purpose consistent with the scope of the Assisting Police Service's program;
- the probe image is of sufficient quality to meet the Assisting Police Service's minimum standards;
- the information shared with the Requesting Police Service will only be used as an investigative lead and will not be shared further without the Assisting Police Service's express agreement;
- the information the Assisting Police Service shares will be permanently destroyed, deleted, or returned by the Requesting Police Service on the earlier of:
  - the information no longer being necessary for the investigation, consistent with the destruction criteria for unidentified probe images set out in Consideration 10 (*Retention of Prove Images*); or
  - the associated mugshot-related records should be purged following the criteria set out in Recommendation 3.2.

[8] Individuals have the right to access and correct their personal information under section 37 of FIPPA and section 36 of MFIPPA. There also exists a general right of access to information for certain groups under section 10 of FIPPA and section 4 of MFIPPA.

## 15. Joint Facial Recognition and Mugshot Database Programs

The IPC notes that **combining FR mugshot databases with other police services may exacerbate privacy risks**. Therefore, proper assessments and consultations should take place, including a joint PIA. Furthermore, any merging initiative should be limited to police services within Ontario, and the police services should create governance frameworks for the joint program based on the Guidance.

***IPC's Recommendations:***

15.1. Each police service involved in a joint FR mugshot database program should consider their lawful authority to do so and follow all the considerations and recommendations in the Guidance, including:

- conducting a joint PIA and other necessary risk assessments
- entering into a formal information-sharing agreement
- establishing related policies, procedures and requirements binding all parties of the joint program to equivalent standards and safeguards consistent with the Guidance

15.2. The information-sharing agreement should clearly limit the use of shared mugshot records to the purposes of:

- a reasonable, necessary, and proportionately scoped program
- conducting and reporting on regular testing, reviews, and audits of the joint program
- preparing a report required by the agreement
- or for a purpose required by law

15.3. Before combining databases, police should review their arrest record policies, record schedules, and mugshot databases, and purge mugshot records that reflect excessive, discriminatory, or unlawful retention practices, including relating to non-conviction arrest records described in Consideration 3 (*Mugshot Database and Related Policies*)

15.4. Each police services board should regularly audit and evaluate the effectiveness and appropriateness of any joint FR mugshot database program and make such reports publicly available.

## C. Program Review Stage

### 16. Ongoing Monitoring and Reassessment

Police should **regularly monitor and assess the operation of the FR mugshot database program and any risks associated with it** to mitigate and limit harms related to potential system errors or bias, misidentification, program deficiencies, security threats, or the misuse or mishandling of sensitive biometric information.

***IPC's Recommendations:***

16.1. Once the FR mugshot database program is in use, regularly monitor and re-assess the performance and privacy risks of your system based on available information, emerging risks, best practices, and broader developments in the use of FR technology.

16.2. Decide whether any existing risk assessments, including the PIA, program policies, procedures, or overall design and operation of the FR mugshot database program or FR system needs to be re-evaluated and updated.

16.3. Consider consulting with the IPC if new impacts or privacy risks arise.

### 17. Accountability

The IPC recommends that police services set and follow ongoing accountability measures.

***The IPC's Advice on Accountability***

The IPC recommends conducting annual compliance audits, which, at a minimum, should assess:

- ongoing compliance with lawful authority and other legal requirements
- ongoing compliance with the program's policies and procedures
- the sufficiency and frequency of updates made to the program's policies and procedures, including updates to public information and reporting about the program
- the methods for reviewing the contents of the mugshot databases to reduce bias and maintain regular purging practices that follow retention rules and requirements
- any public complaints received about the program and how they were handled
- any privacy breaches that occurred and how they were handled
- third-party compliance with the privacy obligations of the program

***IPC's Recommendations:***

17.1. Set and follow ongoing accountability measures, including annual compliance audits, to assess the FR mugshot database program's compliance with legal requirements, rules, policies, and procedures. This should include compliance by any third parties involved in the program and annual program reviews to measure the overall success of the program in achieving its intended purpose and respecting its guiding principles.

17.2. Assess and publicly report on the results of annual compliance audits and program reviews, including by providing the public with annual information and statistics relating to the compliance, effectiveness, and appropriateness of the FR mugshot database program.

Further, the IPC recommends that police services, through their police boards, should conduct **annual program reviews** to determine whether the FR mugshot database program is operating as anticipated and is adhering to its guiding principles. This annual program review should make use of statistics, and at a minimum, these statistics should include:

- information about the size and demographic makeup of the relevant databases
- the number and nature of FR searches performed over the past year, including requests made by other police services
- metrics on the effectiveness of the program, such as the number of investigative leads generated as a result of FR used in connection with mugshot databases, and the number of charges and convictions associated with those leads

## Conclusion

If you are a police service or police services board operating in Ontario who has implemented or is planning to implement FR technology for a mugshot database, then you should begin to update (or develop) policies to ensure compliance with Ontario's access and privacy laws. Reviewing the Checklist provided in Appendix A of this advisory can help verify that your policies and procedures are consistent with the requirements and recommendations found in the Guidance.

# Appendix A
# Checklist: IPC's Recommendations
# For Implementing A Facial Recognition (FR) Mugshot Database Program

| **Pre-Implementation Stage** | | | |
|---|---|---|---|
| | **Recommendations** | **Guidance Ref.** | |
| A. | Clearly document the lawful authority that is being relied on to operate the FR mugshot database program. | 1.1 | ☐ |
| B. | Review the design and proposed operation of the program (including use of third-party service providers) to ensure it meets all relevant legal requirements. | 1.2-1.3 | ☐ |
| C. | Prepare guiding principles for using the program that addresses (i) fair, effective, and equitable policing services; and (ii) the protection and advancement of privacy, transparency, accountability and human rights. | 2.1 - 2.2 | ☐ |
| C.1 | • These principles are publicly available. | | ☐ |
| C.2 | • These principles are adhered to throughout all stages of development of the program. | | ☐ |
| C.3 | • These principles are adhered to throughout all stages of operation of the program. | | ☐ |
| D. | Review applicable arrest record policies and retention schedules to ensure they do not permit or facilitate the excessive, discriminatory, unconstitutional, or otherwise unlawful retention and use of mugshot records. | 3.1 | ☐ |
| E. | Following the review for item D, and on an annual basis going forward, purge mugshot databases of records that reflect or may facilitate excessive, discriminatory, or unlawful police practices, such as (i) non-conviction arrest records; and (ii) arrest records connected to summary offences; and (iii) arrest records for persons dealt with under the Youth Criminal Justice Act (YCJA), after the YCJA access periods have expired. | 3.2 | ☐ |
| E.1 | • A schedule is established for purging records with retention periods of less than one year. | | ☐ |

| | | | |
|---|---|---|---|
| E.2 | • The next annual review is scheduled. | | ☐ |
| F. | Conduct a Privacy Impact Assessment (PIA) and produce a report that addresses the privacy risks of using FR technology along with the safeguards and controls that can be incorporated into the program to mitigate these risks. | 4.1 - 4.2 | ☐ |
| G. | Share your PIA report with your police services board and ensure it (or a summary) be made available to the public. | 4.3 | ☐ |
| H. | Conduct other risk assessments such as security, human rights, and algorithmic impact assessments as needed, and ensure these are combined or coordinated with your PIA. | 4.4 | ☐ |
| H.1 | • Perform a security (threat risk) assessment. | | ☐ |
| H.2 | • Perform a human rights assessment (including checking for bias). | | ☐ |
| H.3 | • Perform an algorithmic impact assessment. | | ☐ |
| H.4 | • Identify and perform any other assessments that should be performed. | | ☐ |
| I. | Establish and limit the scope and purpose of the program by focusing on generating investigative leads for the purpose of identifying individuals reasonably suspected of having committed a serious offence.<br>Ensure to adhere to this scope, comply with applicable law, and follow the privacy principles of reasonableness, necessity, and proportionality. | 5.1 | ☐ |
| J. | Develop and approve comprehensive policies and procedures for the program consistent with the IPC's Guidance on FR databases. | 5.2 | ☐ |
| K. | Carry out public consultations to obtain stakeholder feedback on the program, including addressing privacy and equity concerns associated with communities that are disproportionately affected by systemic discrimination and over-policing practices. | 6.1 – 6.2 | ☐ |
| L. | Post up-to-date, readily available, plain language information about the program on the websites of both the police services board and the police service. | 7.1 | ☐ |

| | | | |
|---|---|---|---|
| L.1 | • The most current version of the program's policies and procedures are posted. | | ☐ |
| L.2 | • Copies of the PIA and other risk assessments (or at lease summaries of these assessments) are posted. | | ☐ |
| L.3 | • A plain language explanation of how the program works, including its scope and purpose, lawful authority, and safeguards and controls is posted. | | ☐ |
| L.4 | • Details on past public consultations, including a general description of the consultees, the nature of the consultation (focus groups, meetings, surveys), and a general summary of the feedback are posted. | | ☐ |
| L.5 | • Information on the procurement of the FR system, including details on third-party service providers and their compliance with privacy obligations, is posted. | | ☐ |
| L.6 | • The results of any testing for accuracy or bias, including a general description of the testing methodology are posted. | | ☐ |
| L.7 | • Statistics measuring the overall effectiveness of the program is posted | | ☐ |
| L.8 | • Information about how individuals can request access to, and correction of their personal information is posted. | | ☐ |
| M. | Carry out a pilot program to test the FR program and ensure its effectiveness in achieving the intended results, identify and address any unintended issues or consequences, and mitigate risks to privacy and human rights. | 8.1 | ☐ |
| M.1 | • The pilot program is designed with the IPC's recommendations and compliance with existing laws in mind. | | ☐ |
| M.2 | • The pilot program is conducted. | | ☐ |
| M.3 | • The results of the pilot program are assessed and, if proceeding beyond the pilot program, a plan for addressing known issues is developed and being implemented. | | ☐ |

| | | | |
|---|---|---|---|
| N. | Evaluate and publicly report on the results of the pilot, including sharing key findings with affected communities and interested parties as part of the public engagement process. | 8.2 | ☐ |
| **Operational Stage** | | | |
| O. | Set and follow clear standards for ensuring minimum photo quality of probe images consistent with the IPC's Guidance on FR databases. | 9.1 | ☐ |
| P. | Set clear rules and processes for retention limits and the secure destruction of probe images (including unidentified probe images). These should be consistent with the IPC's Guidance on FR databases and there should be an oversight process in place to regularly confirm compliance with rules. | 10.1 – 10.2 | ☐ |
| Q. | Take steps to regularly test for bias and inaccuracy in the performance of the FR system. For example, this may include internally evaluating whether system parameters like minimum threshold settings for a match are set appropriately or need to be adjusted to avoid false positives and support program evaluation. | 11.1 | ☐ |
| Q.1 | • Initial testing conducted as part of implementation. | | ☐ |
| Q.2 | • The frequency of testing and its scope is documented. | | ☐ |
| Q.3 | • The next test is scheduled. | | ☐ |
| R. | Set transparent procedures for the human review and accuracy controls of the program. These procedures should outline who is responsible for conducting the review, how trained operators interpret and explain the results of FR searches and the training requirements necessary for the job. Trained operators should follow clear criteria and be able to explain the steps and processes followed for generating investigative leads. | 11.2 | ☐ |
| S. | Develop and implement requirements for documenting all FR searches and assessment results. This documentation should cover the probe image and match threshold that was used, the likelihood of a match, the output as determined by the FR system, the trained operator who conducted the search, the operator's post-assessment decision on whether to treat a potential match as a false positive or a potential investigative lead, and any other relevant information. | 11.3 | ☐ |

| | | | |
|---|---|---|---|
| T. | Ensure your program's policies and procedures set out the requirements and parameters for the collection, retention, use, or disclosure of personal information as it pertains to the different aspects of your program. This includes limiting the collection, retention, use, or disclosure of personal information to what is necessary and proportionate for achieving the stated purpose of your program. | 12.1 – 12.2 | ☐ |
| U. | Adopt comprehensive administrative, technical, and physical controls and safeguards for the collection, retention, use, or disclosure of personal information involved in the program. | 12.3 | ☐ |
| V. | Ensure that there are policies and procedures in place on individuals' rights to access and correct their personal information and expunge their arrest records. These policies and procedures should be written in plain language, be in compliance with applicable law, and made publicly available. | 13.1 – 13.2 | ☐ |
| W. | Set policies and procedures for handling requests from other police services, including:<br>• receiving and processing requests to run FR searches in the mugshot database;<br>• disclosing the results of any potential matches to the requesting police service; and<br>• maintaining detailed records and logs of all access and disclosures of personal information, such as (i) FR search requests received, (ii) whether they were processed and how, (iii) results, and (iv) any information returned to the requesting police service. | 14.1 | ☐ |
| W.1 | • Standard form for requests from other police services is developed, approved and in use. | | ☐ |
| W.2 | • Logs are implemented. | | ☐ |
| W.3 | • Standard form for disclosing results in response to requests is developed, approved and in use. | | ☐ |
| X. | For Joint FR Programs: | 15.1 – 15.4 | ☐ |
| X.1 | • Assessment of reasonableness, need and proportionality is complete | | ☐ |
| X.2 | • Joint policies and procedures to support compliance with law and the IPC's recommendations are in place. | | ☐ |
| X.3 | • PIA is completed. | | ☐ |

| | | | |
|---|---|---|---|
| X.4 | • Testing and auditing scope and frequency is documented. The next test is scheduled. The next audit is scheduled. | | ☐ |
| X.5 | • Information sharing agreement is in place.<br>• The information-sharing agreement should clearly limit the use of shared mugshot records for the purposes of:<br>• a reasonable, necessary, and proportionately scoped program, (e.g., it focuses on only generating investigative leads for serious crimes);<br>• conducting and reporting on regular testing, reviews and audits of the joint program;<br>• preparing a report required by the agreement; or<br>• for a purpose required by law. | | ☐ |
| X.6 | • Before combining databases, each police service should review its arrest record policies, record schedules, and mugshot databases in an effort to purge mugshot records that reflect excessive, discriminatory, or unlawful retention practices, including in relation to non-conviction arrest records. | | ☐ |
| **Program Review** | | | |
| Y. | Regularly monitor and assess the performance and privacy risks of your program system based on available information, best practices, and the developing FR technology landscape. This includes determining whether any existing risk assessments (e.g., PIA), policies, procedures, or the overall design and operation of the program or FR system should be re-evaluated and updated.<br>The IPC recommends considering consulting it if new impacts or privacy risks arise. | 16.1 – 16.3 | ☐ |
| Z. | Implement ongoing accountability measures, including annual compliance audits, to assess the program's compliance with legal requirements, rules, policies, and procedures. Such review should consider compliance by any third parties involved in the program.<br>Also, conduct annual program reviews to measure the overall success of the program in achieving its intended purpose and respecting its guiding principles.<br>Reports on the results of annual compliance audits and program reviews should be made available to the public. | 17.1 – 17.2 | ☐ |
| Z.1 | • The annual compliance audits are scheduled. | | ☐ |