JANUARY 2024

Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

Facial Recognition and Mugshot Databases: Guidance for Police in Ontario

This guidance by the Office of the Information and Privacy Commissioner of Ontario (IPC) is intended to enhance understanding of rights and obligations under Ontario's access and privacy laws respecting police use of facial recognition technology in connection with mugshot databases. It should not be relied upon as a substitute for the legislation itself or as legal advice. It does not bind the IPC's Tribunal that may be called upon to independently investigate and decide upon an individual complaint or appeal based on the specific facts and unique circumstances of a given case. For the most up-to-date version of this guidance, visit **www.ipc.on.ca**.

Acknowledgement

The IPC shared a draft of this guidance with a number of interested parties, including:

- Academics
- Civil society and human rights organizations
- Criminal defense, legal aid and lawyers' organizations
- Members of the IPC's Strategic Advisory Council
- Municipal police services
- Provincial government ministries
- Privacy, human rights, and law commissions

The IPC appreciates the thoughtful comments provided by these organizations and individuals.

Contents

Section 1 – Introduction

Background

In May 2022, the Information and Privacy Commissioner of Ontario (IPC) joined with federal, provincial, and territorial counterparts across Canada (FPT commissioners) to issue a **joint statement** calling for a clear, comprehensive legal framework to address the risks to privacy and other fundamental rights related to police use of facial recognition technology in Canada.[1] In the meantime, they released **privacy guidance** to clarify police privacy obligations under current laws and to help ensure that any use of facial recognition minimizes privacy risks and respects privacy rights.[2]

Police services in Ontario have begun using facial recognition technology, among other biometric technologies, to carry out public safety initiatives more efficiently. When used responsibly, facial recognition technology used in connection with mugshot databases may help police identify investigative leads.

Facial recognition (FR) is an artificial intelligence (AI) technology that collects and processes sensitive personal information to identify or verify an individual's identity. FR uses image processing software to analyze an individual's facial features, such as the width of the nose, the length of the jawline, and the distance between the eyes (e.g., as they appear in a photograph). **FR algorithms** turn facial features into a **faceprint** of an individual. A facial recognition system can then compare two faceprints and return a **simlarity score** or match faceprints by searching a reference database of a large number of images for a list of potential candidates whose similarity score is at, or above, a given **threshold**.

Police-operated mugshot databases consist primarily of mugshot records, including photographs, also known as booking images, of individuals who have been charged with **serious crimes**. Using FR on mugshot databases can improve the police's ability to identify unknown individuals by improving the speed and scale of **identification**.

Despite the intended benefits of facial recognition systems, the technology raises significant legal, privacy, and ethical challenges given its potential to provide biased or inaccurate results and undermine rights and freedoms. Jurisdictions around the world continue to struggle with how to regulate its use.[3]

1 See the joint statement by Federal, Provincial and Territorial (FPT) Privacy Commissioners on the **Recommended legal framework for police agencies' use of facial recognition.**

2 See the **joint statement by the Information and Privacy Commissioner of Ontario and the Ontario Human Rights Commission on the use of AI technologies**.

3 See the Citizen Lab and the University of Toronto, International Human Rights Program's **To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada**.

In addition, members of the public, civil society, government, and academia have expressed their concerns about the general risks associated with the use of facial recognition, including:

- risks to privacy and other fundamental rights, including the right to equality and non-discrimination, such as:
    - gender and race-related bias and inaccuracy
    - system or human errors that can lead to individual consequences, such as undue or excessive scrutiny or suspicion, or being subject to wrongful detention, arrests, or charges
    - over-policing of low-income, Black, Indigenous, and other marginalized communities
- a lack of transparency, accountability, and oversight of the organizations adopting FR
- the potential misuse, manipulation, and unauthorized access to individuals' **biometric information**

At the time of publication of this guidance, the lawfulness of police facial recognition mugshot programs, including compliance with the *Canadian Charter of Rights and Freedoms* (the Charter), has yet to be addressed by the courts or a tribunal. Meanwhile, there is no clear or comprehensive set of legal rules in effect in Ontario governing police use of facial recognition technology, including for mugshot database programs. While the *Identification of Criminals Act* (ICA) permits police to photograph individuals charged with serious crimes and compile related information for law enforcement purposes, the act does not address the use of facial recognition technology, AI technology, biometrics, or biometric databases. The act also does not address what safeguards or controls are required to ensure necessary, proportionate, and non-discriminatory police FR mugshot practices. This leaves gaps in the current law, which, if left unaddressed, risk serious harms to individuals' right to privacy and other fundamental human rights.

Scope of guidance

This Ontario-specific guidance for police use of facial recognition in connection with mugshot databases builds on the FPT guidance of May 2022. During provincial consultations on proposed FPT guidance, Ontario police services and other groups identified the need for more practical regulatory guidance on specific use cases of FR by police. **In response, this guidance addresses the specific use case of facial recognition software use by police to identify individuals using a mugshot database in Ontario.**

The terms "facial recognition mugshot database program," "FR mugshot database programs" and "programs" are used interchangeably throughout this guidance to refer to this specific application.

The guidance provides recommendations to help reduce specific risks associated with FR mugshot database programs. It includes key privacy, transparency, and accountability-related

considerations to design, use, and govern such programs responsibly. It also has a glossary of terms and a summary of recommendations in the appendices.

Purpose of guidance

The IPC developed this guidance to help Ontario police services and police services boards (police)[4] meet their obligations under Ontario's access and privacy laws. The guidance should be used by police that are considering setting up a facial recognition mugshot database program, including any joint programs. The guidance also applies to police that have already started using facial recognition for these types of programs. The IPC recommends that police commit to reviewing their current programs against this guidance as soon as possible.

This guidance is not an endorsement of the use of facial recognition technology to improve or accelerate searches of mugshot databases. It acknowledges that using facial recognition on mugshot databases is not without risks. This guidance also does not replace the need to have a broader debate about how laws should be updated to govern police use of facial recognition more effectively. Rather, it is intended to contribute to discussion and decision-making about whether and how police may responsibly use facial recognition in connection with mugshot databases while respecting the rights of persons and diverse groups in Ontario. Like other advanced AI technologies, public sector use of facial recognition in Ontario needs to be built on clear and binding guardrails that effectively address safety, privacy, accountability, transparency, and human rights.[5]

The following are recommended steps to take before, during, and after implementing an FR mugshot database program. However, police may need to put in place additional privacy protections depending on the nature, complexity, and scope of risks posed by their specific program.

4 Where this guidance refers to police service boards, it should be read as including requirements for both police services boards and the Solicitor General who oversees the Ontario Provincial Police.

5 See the **joint statement by the Information and Privacy Commissioner of Ontario and the Ontario Human Rights Commission on the use of AI technologies**.

Section 2 – Pre-implementation: key policy and legal considerations

When considering the privacy impacts of a proposed technology program, such as the use of facial recognition in connection with mugshot databases, police should assess whether the benefits will clearly outweigh the risks. They should also consider if the program is necessary and proportionate in the circumstances before deciding how to use the technology in a manner that respects privacy and human rights. The following are key considerations to address during the planning, development, and testing stages before operating an FR mugshot database program.

Key consideration 1: lawful authority and lawful operation

The goal of identifying individuals who are reasonably suspected of having committed a serious offence is a legitimate law enforcement purpose. That said, FR mugshot database programs impact the reasonable expectation of privacy of individuals, particularly individuals whose mugshots the police retain and use in a mugshot database after their charges have been dismissed or withdrawn.

In this context, questions arise about the source and scope of police powers to create, store, and use biometric faceprints in mugshot databases and the absence of adequate safeguards and controls. In these circumstances, a carefully considered, incremental, transparent, and accountable approach to using facial recognition is necessary to ensure public trust. Providing the public with information about the source and scope of the lawful authority to act is particularly important where there is legal uncertainty and significant concerns about the adequacy of safeguards and controls.

Police have a duty to ensure that they have lawful authority and are acting lawfully. To ensure lawful authority for the design and operation of an FR mugshot database program in Ontario, police should consider the following key factors:

- A facial recognition mugshot database program involves the collection, retention, use, and disclosure of personal information and must comply with the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).
- The creation of faceprints generally involves collecting new and sensitive personal biometric information, separate and apart from any photographs used in creating that biometric information.[6]
- FIPPA and MFIPPA permit police to collect, retain, and use personal information and to disclose this information to each other for legitimate law enforcement purposes. However, where the collection, retention, use, or disclosure of personal information attracts a reasonable expectation of privacy, it must be independently authorized

6 See IPC **Investigation PC-010005-1**, into the Alcohol and Gaming Commission of Ontario's use of facial recognition technology in Ontario casinos; the British Columbia Information and Privacy Commissioner (B.C.I.P.C.) **Investigation Report F12-01** into the use of facial recognition technology by the Insurance Corporation of British Columbia; **PIPEDA Findings #2020-004**, into the Cadillac Fairview investigation; **PIPEDA Findings #2021-001** into the Clearview AI investigation; and B.C.I.P.C **Investigation Report 23-02** into Canadian Tire Associate Dealers' use of facial recognition technology.

under common law or statute.[7] In addition, police are generally not permitted to collect, retain, or use personal information that was collected or compiled by another law enforcement agency, institution, or a third-party service provider contrary to law.[8]

- Canadian courts have held that the collection, retention, use, and disclosure of non-conviction arrest records under the *Identification of Criminals Act* (ICA), such as mugshots and fingerprints, attract a diminished, but nonetheless, reasonable expectation of privacy within the meaning of section 8 of the Charter.[9]
- A facial recognition mugshot database program must comply with *Ontario's Human Rights Code* and the Charter, including the privacy rights protected under section 7 and section 8 and the equality rights protected under section 15. Charter and human rights analyses should consider and address the long-standing concerns about disproportionate policing practices vis a vis Indigenous, racialized, and other marginalized communities and the ways they may be overrepresented in the collection of faceprints and their retention and use in mugshot databases.[10] The necessity and proportionality analysis of a facial recognition mugshot database program will also be relevant under section 1 of the Charter.
- The ICA authorizes the identification of certain individuals using "measurements, processes and operations of fingerprinting, palm printing and photography". However, the ICA does not refer explicitly to facial recognition or facial recognition-augmented databases. Police who assume that the ICA authorizes the creation and comparison of faceprints in biometric databases are advised to carefully review the scope of their authority and ensure that they have rigorous safeguards and controls in place. [11]
- Even if a court or tribunal eventually determines that the ICA or some other law authorizes the creation and comparison of faceprints in biometric databases, authority derived under the ICA for collecting mugshots is limited to those individuals charged with serious crimes, and ICA authority for retaining mugshots is limited to what is necessary and proportionate.

---

7 See **R. v. Orlandis-Habsburgo**, 2017 ONCA 649 (CanLII), **R. v. Spencer**, 2014 SCC 43, [2014] 2 S.C.R. 212; **R. v. El-Azrak**, 2018 ONSC 4450 (CanLII); **R. v. Otto**, 2019 ONSC 2514 (CanLII); **R. v. Marakah**, 2017 SCC 59 (CanLII), [2017] 2 SCR 608; and **R. v. Jones**, 2017 SCC 60 (CanLII), [2017] 2 SCR 696.

8 See IPC **MO-2225**; IPC **PO-2826** and the Office of the Privacy Commissioner of Canada's Special Report: **Police use of Facial Recognition Technology in Canada and the way forward** on the investigation into the RCMP's use of Clearview AI.

9 See **R. v. Beare; R. v. Higgins**, 1988 CanLII 126 (SCC), R. v. Doré, [2002] O.J. No. 2845 (OCA), Lin v. Toronto Police Services Board, [2004] O.J. No. 170 (Ont. Sup. Ct.), **R. v. Strickland**, 2017 BCPC 1 (CanLII), and **R. v. Strickland**, 2017 BCPC 211 (CanLII), **R. v M.O.**, 2017 ONSC 1213 (CanLII), and **R. v. Fogah-Pierre**, [2023] O.J. No. 1999 (ONSC).

10 See for example, **R. v. Le**, 2019 SCC 34 (CanLII); the Ontario Human Rights Commission's Second Interim Report, **A Disparate Impact** and its Final Report, **From Impact to Action**; the information on Toronto Police Service's **Race and Identity-Based Data Collection;** and the August 26, 2022 **Toronto Star article** on disproportionality-related data from Peel Regional Police.

11 Note that in Beare, the Supreme Court of Canada held that the ICA does not "grant unlimited powers to use unrestricted methods to establish identity. Only processes which have been sanctioned by the Governor in Council are authorized." In addition, the Court observed that the ICA provides for "publication of the results of tests for the purpose of affording information for those engaged in the execution or administration of the law, but I do not think it authorizes their unconstitutional retention."

- Agreements between police and any third-party vendors or commercial service providers of facial recognition technology should contain terms and conditions that ensure compliance with laws applicable to police in Ontario, including restrictions on the collection, access to, retention, use, and subsequent disclosure of personal information. Third-party vendors or commercial service providers and their products must also comply with applicable private-sector privacy laws, including the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

Recommendations:

1.1 Ensure you have lawful authority to operate a facial recognition mugshot database program and your authority is clearly documented before you start the program. If you are already operating a program, re-evaluate lawful authority as soon as possible.

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

1.3 If there are any gaps in lawful authority, legal compliance, or rights protections, you should adjust the scope of the FR mugshot database program to ensure compliance with the law and the protection of fundamental rights.

Key consideration 2: guiding principles

To help ensure public trust, police should develop and publicly communicate the principles that will guide their decisions and actions when using facial recognition technology in connection with mugshot databases. Public trust and community acceptance of a program will depend on the transparency of the guiding principles and a demonstrated commitment to respect and uphold them.

At a minimum, a statement of principles should commit to using facial recognition in a way that:

- 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

Recommendations:

2.1 Draft and publicly communicate a statement of guiding principles for the use of FR in connection with mugshot databases 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 a facial recognition mugshot database program.

Key consideration 3: mugshot databases and related policies

The responsible design and operation of your FR mugshot database program require that the program be structured and governed to account for the underlying information environment in which the program will be deployed.

Policing leaders should consider the growing body of evidence that arrest records contained within a mugshot database program may be associated with discriminatory or disproportionate policing[12] and continue to take up their responsibilities to reverse the impact of these historical and current police practices. When operating or considering developing an FR mugshot database program, police must assess and address the extent to which investigative practices and the contents of mugshot databases reflect discriminatory investigative, arrest, and charging practices. A critical component of this work relates to establishing appropriate mugshot records retention and destruction requirements.

With a few limited and narrow exceptions, there are no statutory retention or destruction requirements for personal information collected under the ICA.[13] Instead, the responsibility for setting such rules and requirements is left to the discretion of those responsible for establishing record retention schedules, effectively police services boards.

In exercising their responsibilities to put in place records retention and destruction rules and requirements, police services boards should ensure that police retain mugshot records only for as long as is necessary and proportionate. At a minimum, the relevant rules, requirements, and processes should recognize and protect the privacy and

12 See for example, **R. v. Le**, 2019 SCC 34 (CanLII); the Ontario Human Rights Commission's Second Interim Report, **A Disparate Impact** and its Final Report, **From Impact to Action**; the information on Toronto Police Service's **Race and Identity-Based Data Collection;** and the August 26, 2022 **Toronto Star article** on disproportionality-related data from Peel Regional Police.

13 The only exception to this is the requirements in sections 4 and 5 of the *Identification of Criminals Act* which mandate the destruction of fingerprints and photographs for offences dealt with under the *Contraventions Act* and *Cannabis Act* by way of a ticket.

equality rights of young people, racialized and Indigenous persons, and other vulnerable individuals and communities.

In addition, individuals who have never been convicted of a serious crime and do not face any current charges or proceedings should be protected against the excessive retention and use of their personal information, particularly as compiled in searchable mugshot databases. This requires that police update their mugshot databases to ensure that they accurately reflect the final disposition of criminal charges,[14] and purge their mugshot databases of:

- non-conviction arrest records
- arrest records tied to summary offences, including hybrid offences[15] after the Crown has elected to proceed on a summary basis and
- arrest records of persons dealt with under the *Youth Criminal Justice Act* (YCJA), after the YCJA access periods have expired[16]

Purging records from mugshot databases should be completed as soon as reasonably practical, with consideration for the need to retain records associated with linked cases or appeals. Exceptions to mugshot database purging requirements should only be permitted in highly limited circumstances. Police should clearly define these circumstances in police policies, procedures, records schedules, and other directives. The criteria or factors used to define these circumstances must be consistent with the laws described above, in **key consideration 1**. When applying the criteria to an individual case, the decision should be documented and reviewed as part of **annual compliance audits**.

Recommendations:

3.1 Before putting in place an FR mugshot database program, review arrest record policies and retention schedules, particularly those governing mugshot databases, to ensure they do not permit or facilitate the excessive, discriminatory, unconstitutional, or otherwise unlawful retention and use of mugshot records.

3.2 Before putting in place an FR mugshot database program, and on an annual basis moving forward, purge mugshot databases of records that reflect or may facilitate excessive, discriminatory, or unlawful police practices, including by purging:

- non-conviction arrest records
- arrest records tied to summary offences, including hybrid offences after the Crown has elected to proceed on a summary basis and

14 See **Shanthakumar v. CBSA**, 2023 ONSC 3180 (CanLII).

15 For more information regarding hybrid and summary offences, see the definition of serious crime in the **Glossary** of this guidance document.

16 See **R. v. Fogah-Pierre**, [2023] O.J. No. 1999 (ONSC) which makes it clear that youth records are to be routinely destroyed or at the very least, restricted such that no one, including police, can access them once the access periods set out in section 119 of the Youth Criminal Justice Act have ended.

- arrest records of persons dealt with under the *Youth Criminal Justice Act* (YCJA), after the YCJA access periods have expired

3.3 If you are currently operating an FR mugshot database program, review and purge mugshot records consistent with recommendations 3.1 and 3.2, starting as soon as reasonably practical but no later than one year following the release of this guidance and on at least an annual basis moving forward.

Key consideration 4: privacy impact assessments

Facial recognition mugshot database programs raise significant privacy risks related to how biometric facial data and other personal information may be collected, used, disclosed, and retained. These risks include the potential misuse of personal information, potential bias and inaccuracy, and technological or human errors that could result in false recognitions, wrongful arrests, and other types of intrusive investigative scrutiny.

You should assess, reduce, and monitor these and other risks throughout your program's lifecycle. Privacy safeguards and controls must be in place at the outset of your program's design and development to protect personal information, including **training data**, biometric faceprints, probe images, mugshot databases, and information gathered from FR searches.

Widely recognized as a best practice, privacy impact assessments (PIAs) are a risk management tool that helps institutions assess the potential privacy risks of a program or activity.[17] PIAs can also help identify the basis and extent of your lawful authority, improve transparency, and meet your privacy obligations under the law. To assist in understanding privacy risks, obligations and mitigation measures, consult with relevant privacy experts early in the PIA process.

Your PIA process should be documented in a PIA report. The PIA report should address all privacy risks and explain the related risk mitigation strategies, including those required to protect the privacy rights of individuals and communities whose personal information may be collected, retained, used, or disclosed in probe images and mugshot records. Risk mitigation strategies should include:

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

PIAs should also reflect that FR mugshot database programs:

- involve the collection of new and sensitive personal biometric information, separate from any photographs used in the creation of that biometric information[18]

17 For more information on PIAs, see the IPC's **Planning for Success: Privacy Impact Assessment Guide**.

18 See IPC **Investigation PC-010005-1**, into the Alcohol and Gaming Commission of Ontario's use of facial recognition technology in Ontario casinos; the British Columbia Information and Privacy Commissioner (B.C.I.P.C.)

- impact the privacy of all individuals whose personal information may be implicated in the operation of a facial recognition system, not just the individuals whose images are returned as a potential match
- 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 (e.g., in criminal investigation files)
- may facilitate the disclosure of personal information to police in Ontario and other law enforcement agencies in Canada or other countries

You will likely also need to conduct other risk assessments to identify and mitigate security threats, human rights concerns, and AI technology risks, including those related to software and third-party service providers. This may require consultation with relevant experts. These assessments should be combined or coordinated with your PIA.

Recommendations:

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

4.2 Your PIA report should identify and address the privacy risks of using facial recognition technology in the mugshot database context (e.g., as described above) and include safeguards and controls that can be built into the program's policies and procedures to mitigate these risks.

4.3 Share the results of your PIA with your police services board and make the PIA report, or a summary of it, 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 your PIA.

Investigation Report F12-01 into the use of facial recognition technology by the Insurance Corporation of British Columbia; **PIPEDA Findings #2020-004**, into the Cadillac Fairview investigation; **PIPEDA Findings #2021-001** into the Clearview AI investigation; and B.C.I.P.C **Investigation Report 23-02** into Canadian Tire Associate Dealers' use of facial recognition technology.

Key consideration 5: scope, purpose, and program policies

Program scope and purpose

To manage your FR mugshot database program responsibly, you should define and limit the program's scope and purpose. Having a clearly defined scope and purpose will help ensure that the privacy principles of reasonableness, necessity, and proportionality[19] will operate to reduce privacy risks. A well-defined program scope and purpose can also help avoid scope creep, such as deploying facial recognition capabilities as an add-on to other police surveillance technologies.

A reasonable, necessary, and proportionately scoped program should focus on generating investigative leads for the purpose of identifying individuals who are reasonably suspected of having committed a serious offence.

Program policies and procedures

Once the scope and purpose of your program are clearly defined, you should develop and approve comprehensive policies and procedures consistent with the recommendations in this guidance. Including a glossary of definitions and key terms specific to your program in your policies and procedures will ensure a consistent understanding of technical components and processes among staff.

Recommendations:

5.1 Establish and limit the scope and purpose of your FR mugshot database program from the beginning, by focusing on generating investigative leads for the purpose of identifying individuals reasonably suspected of having committed a serious offence. Ensure the scope and purpose are maintained over time and comply with applicable law and the privacy principles of reasonableness, necessity, and proportionality.

5.2 Develop and approve comprehensive policies and procedures for your FR mugshot database program consistent with the recommendations in this guidance.

Key consideration 6: public engagement

Public engagement activities should begin during the earliest stages of the program's development, including before a pilot program. These activities should be timely, informative, and include opportunities for two-way dialogue about privacy and equity concerns with community members and subject matter experts. You should also engage with affected communities and interested parties, particularly over-policed groups such as individuals from Indigenous, racialized, and other marginalized communities.

19 For more information on these privacy principles within the context of police use of facial recognition, see the joint guidance by the FPT Privacy Commissioners on **Privacy Guidance on Facial Recognition for Police agencies**.

You should consult the public on how you will use FR and protect fundamental rights, including the rights of those whose personal information may be contained in mugshot databases and the demographic makeup of such databases. Public engagement may require multiple phases to be meaningful, including sharing important information and updates, asking for feedback, answering questions, and engaging in critical dialogue. In the case of current or ongoing programs, public consultations should still occur even if you have not started this engagement work during the early stages of your program's development.

Ultimately, consulting with affected communities and interested parties and publicly showing you have anticipated and assessed the broader privacy and human rights issues raised by facial recognition *before* putting your program in place will promote accountability and transparency.

Recommendations:

6.1 Conduct meaningful public consultations with affected communities and interested parties about your program before putting it in place. In the case of current or ongoing programs, public consultations should still occur.

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

Key consideration 7: transparency

Well before implementing a FR mugshot database program, you should be transparent with the public about your plans and the evolving nature of the program. Being transparent from the outset will help ensure public trust, including with vulnerable and over-policed communities. Transparency considerations are raised throughout this document and are not limited to this section.

Recommendations:

7.1 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 to foster ongoing transparency.

This public information should include:

- 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 your 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 facial recognition 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
- information about how individuals can request access to and correction of their personal information

Key consideration 8: pilot programs

If you decide to proceed with an FR mugshot database program, you should conduct a time-limited pilot program with clear goals and objectives before full implementation of the technology. An evaluation of the results of the pilot will assist you in making any necessary adjustments to key components of your program, including the PIA, program policies and procedures.

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

- whether the intended benefits of the system are realized and whether any unforeseen risks or harms have appeared
- whether FR search requests and procedures are being followed correctly, including the effective documentation of search results (see **key consideration 11** for further details on documentation)
- whether staff using the FR system have been effectively trained 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, for example to avoid **false positives** and support program evaluation
- whether there is any evidence of errors, inaccuracy, or bias in system outputs or in staff or officer interpretation of those outputs

Following an evaluation of the pilot program, consultees should be updated with its key findings as part of a meaningful public engagement process.

Recommendations:

8.1 Conduct a time-limited pilot program with clear goals and objectives before fully implementing the 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.

Section 3 – Key operational considerations

Key consideration 9: quality of probe images

Probe images are often collected by police during criminal investigations. These images can vary in quality. To support the lawful and accurate use of FR, reduce the risks of misidentification, and assist with your program's review and evaluation, you should set minimum standards for the quality of probe images. Specifically:

- Set 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 facial recognition system's search results. These standards should be used to support rather than replace the judgement of trained operators. In addition, these standards should be used to support the effective and objective review and evaluation of your FR mugshot database program.
- Avoid the use of artist or composite drawings or photos of lookalike individuals as probe images. Studies have shown that facial recognition systems perform poorly on composite sketches, with a greater risk of misidentifying individuals and returning poor search results.[20]
- Avoid digitally altering probe images. If altering an image is justified, (for example, when having to blur or remove the faces of other individuals in the background to protect their privacy), document any steps taken to alter it.

Recommendations:

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

20 See Georgetown Law Center on Privacy and Technology's **Garbage In, Garbage Out. Face Recognition on Flawed Data**.

Key consideration 10: retention of probe images

To minimize infringement of privacy rights, you should ensure that your FR mugshot database program does not automatically save, store, or retain probe images after running a facial recognition search. Retain the original probe image only as long as necessary, for example, to preserve evidence in a criminal proceeding. Specific probe images that become evidence in a criminal proceeding may be subject to additional retention requirements under the rules of evidence, which are beyond the scope of this guidance.

Some probe images will not register a match when searched against a mugshot database. These are known as unidentified probe images. These too should not be retained for longer than necessary. Unless their continued retention is required by law or for the proper administration of justice, 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)

You may need to retain probe images (including unidentified probe images) for longer than would otherwise be appropriate to run internal testing of your FR system's performance. Any retention of probe images for testing purposes should be limited to what is strictly necessary to meet accuracy or other performance requirements for your program. Images retained for testing purposes should be immediately destroyed once testing is completed.

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. These should be consistent with the circumstances described in this guidance.

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

Key consideration 11: accuracy, human review and oversight of results

To ensure accuracy, fairness, bias-free service delivery and the overall effectiveness of your program, you should document and explain how you will interpret and act on the results of FR searches. Testing and human oversight of these programs is essential to

prevent overreliance on potentially faulty algorithms. Failure to carefully review the search results or placing too much confidence in them could result in the unnecessary or unfair investigation of an individual.

Accuracy

You should not assume the accuracy of FR software and the results generated by your FR system. FR systems can vary in quality, reliability and accuracy rates. Research has shown that racialized individuals and women are more likely to be misidentified by facial recognition technology.[21] In addition, the performance of FR systems tends to decline for images that are more than five years old.[22]

You will need to take steps to minimize inaccuracy and bias in the performance of your FR system as a whole. This should include internally evaluating whether system parameters, such as minimum threshold settings for a match are set appropriately or need to be adjusted, for example, to avoid false positives and support program evaluation.

A match between a probe image and a faceprint in a mugshot database will generally be assessed against a pre-established threshold (e.g., a specific similarity score or a predetermined number of potential matches). Selecting an appropriate threshold will depend on the nature and scope of your program. In setting an appropriate threshold, you must consider, identify, and mitigate risks to the rights and freedoms of individuals, including those belonging to groups associated with high false positive rates.

Trained operators

Only police staff who are trained operators of the FR system and who follow required policies and procedures should conduct facial recognition searches and reviews on behalf of requesting investigators.

Trained operators with the right expertise should determine whether there is a reasonable possibility for a potential match between a probe image and a mugshot image. Operators should be able to override search results returned by the FR system based on best practices for reducing errors and minimizing bias and inaccuracy.[23]

Even with high probability that a given match generated by the FR system is accurate, results should always be reviewed by trained operators as a safeguard. **Resulting candidate matches should only be treated as investigative leads, and not as a positive identification of an individual.**

---

21 See the Citizen Lab and the University of Toronto, International Human Rights Program's **To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada**.

22 See the New Scientist article on **Face recognition struggles to recognize us after five years of ageing**.

23 For more information on accuracy considerations, see the joint guidance by the FPT Privacy Commissioners on **Privacy Guidance on Facial Recognition for Police agencies**.

Oversight of results

Trained operators and senior staff responsible for the FR system should be accountable for their decisions and actions when using facial recognition. Both operators and senior staff should actively work to reduce the overall risks of inaccurate and biased results and explain how that is being done.

Recommendations:

11.1 Take steps to test for bias and inaccuracy in the performance of the FR system as a whole, 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, for example to avoid false positives and support program evaluation.

11.2 Set and follow transparent procedures for the human review and accuracy controls of your 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 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.

Key consideration 12: limited collection, retention, use, or disclosure of personal information and reasonable safeguards

Your policies and procedures should ensure that any collection, retention, use, or disclosure of records related to your FR mugshot database program is limited and consistent with the law.[24]

As outlined in **key consideration 1**, police forces in Ontario may only collect, retain, use, or disclose personal information under the rules of FIPPA and MFIPPA, as relevant to their police service. The collection, retention, use, or disclosure of personal information that attracts a reasonable expectation of privacy must be independently authorized under common law or a statute and will require an assessment of lawful authority. Special

24 A record is defined in section 2 of both FIPPA and MFIPPA to mean "any record of information however recorded, whether in printed form, on film, by electronic means or otherwise."

attention should be paid to limiting the collection, retention, use, or disclosure of biometric information, given its sensitivity compared to other types of personal information.

In addition, you must ensure that reasonable security measures are in place to protect the personal information within your custody or control. This should include comprehensive administrative, technical, and physical controls and safeguards for the collection, retention, use, or disclosure of personal information.

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 your 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 different parts of your 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.

Key consideration 13: access, correction, and expungement rights

With limited and specific exceptions, individuals whose personal information is in your custody or control have a right to access and correct their personal information under section 47 of FIPPA and section 36 of MFIPPA. The general public, civil society groups, journalists, and others also have a general right of access to information under section 10 of FIPPA and section 4 of MFIPPA. Accordingly, you must have processes in place to respond to access requests and help individuals or their representatives exercise their access rights while complying with privacy requirements.

Additionally, individuals charged with a criminal offence have a common law right to request that their mugshots and other arrest records be expunged once their charges have been disposed of through a non-conviction disposition. In the absence of well-defined and justifiable exceptional circumstances, police must grant such expungement requests.

Recommendations:

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

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

Key consideration 14: requests from other police services

There may be instances when you are asked to run a facial recognition search with a probe image on behalf of another police service to see if an unknown suspect can be identified in your mugshot database. To ensure accountability in these situations, you should create a standard form for use by the requesting police service that outlines the necessary terms and conditions to be met before you decide whether to approve the request, including:

- the request for a probe image search is submitted in writing (e.g., a form with the officer's name, badge number and contact information, the police service, date, details of the information being requested, and investigation number)
- the request is for a purpose consistent with the scope of your program (e.g., it relates to the investigation of a serious crime)
- the probe image is of sufficient quality to meet your minimum standards (see **key consideration 9**)
- the information you share with the requesting police service will only be used as an investigative lead and will not be shared further without your express agreement
- the information you share will be permanently destroyed, deleted, or returned by the requesting police service as soon as either of the following applies:
    - the information is no longer necessary for the investigation, consistent with the destruction criteria for unidentified probe images set out in **key consideration 10** or
    - the associated mugshot-related records should be purged following the criteria set out in **recommendation 3.2**.

You should maintain detailed records of any requests you receive from other police services and how you respond to those requests. This will ensure accountability and oversight, including for auditing and public reporting purposes.

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 other police services to run FR searches in your 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, such as FR search requests received, whether they were processed and how, their results, and the information returned to the requesting police service, if any

Key consideration 15: joint facial recognition mugshot database programs

Some police services in Ontario are considering combining their mugshot databases with that of others to enhance their collective ability to use FR to generate investigative leads. This would result in a joint facial recognition mugshot database program. This guidance also applies to any existing or potential joint programs.

Combining mugshot databases for the purpose of FR should be handled with additional caution as it can exacerbate the privacy and human rights risks of standalone programs. Consult with your subject matter experts, legal services, and the public when considering if a joint program is necessary and proportionate.

Assuming you have lawful authority to proceed, any initiative to combine mugshot databases should be limited to Ontario police services, at least until a clear and comprehensive legal framework for FR exists in Canada.

After conducting a joint PIA and other necessary risk assessments, police services boards and police services should work together to develop equivalent governance frameworks for all parties to a joint program, based on this guidance. This framework should include formal information-sharing agreements and related policies, procedures, and requirements binding the parties. Agreements should clearly limit police to using the shared mugshot records only for the purpose of a reasonable, necessary, and proportionately scoped program, running regular audits of the joint program, preparing a report required by the agreement, or for a purpose required by law.

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 this 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 this 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, (e.g., it focuses on only generating investigative leads for serious crimes)
- 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 in relation to non-conviction arrest records set out in key consideration 3.

15.4 Each police services board involved should regularly audit and evaluate the effectiveness and appropriateness of any joint program and make audit reports and evaluations publicly available.

Section 4 – Program review and evaluation

Key consideration 16: ongoing monitoring and reassessment

Like other AI technologies, facial recognition used in connection with mugshot databases offers new opportunities for law enforcement and new challenges that require monitoring and reassessment. Monitoring and reassessment help maximize the potential for the technology to be operated in the most trustworthy and safe manner possible throughout its lifecycle.[25] If you put in place an FR mugshot database program, you should regularly monitor the performance and privacy risks of the FR system, along with any new developments in the use of FR technology. You should adjust your practices depending on your monitoring results and any new information, emerging risks and best practices. In doing so, you can 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, which may result in having to re-evaluate and update the design and use of your program or FR system.[26]

You should also review your PIA and any other completed risk assessments to confirm whether risks have been effectively reduced and if any unforeseen impacts have arisen. Where there are new impacts or risks, your PIA and program policies and procedures should be updated or re-evaluated accordingly. You should also consider consulting with the IPC if significant new risks or impacts arise.

25 See the World Economic Forum's Insight Report: **A policy framework for responsible limits on Facial Recognition. Use Case: Law Enforcement Investigations**.

26 See the Organisation for Economic Co-Operation and Development (OECD)'s Chapter on **The Technical Landscape** in the book, Artificial Intelligence in Society.

Recommendations:

16.1 Once your 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 facial recognition technology.

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

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

Key consideration 17: accountability

To demonstrate compliance and ensure ongoing public accountability, internal or external experts should run annual compliance audits of your FR mugshot database program.[27] At a minimum, compliance audits should assess:

- ongoing compliance with lawful authority and other legal requirements
- ongoing compliance with your program's policies and procedures
- the sufficiency and frequency of updates made to your 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 your program and how they were handled
- any privacy breaches that occurred and how they were handled
- third-party compliance with the privacy obligations of your program

Police services, through their police services boards, should also conduct annual program reviews to measure the overall effectiveness of their FR mugshot database program, including whether it is achieving the intended purpose and following the guiding principles. Program reviews should make use of demonstrable criteria, such as key statistics. At a minimum, these annual statistics should include:

- information about the size and demographic makeup of the relevant databases, including in relation to the categories of records described in section 3.2 (non-conviction, summary, and Youth Criminal Justice Act records)
- the number and nature of FR searches performed over the past year, including requests made by other police services

27 A police service or its board may wish to consider an independent third party to perform the compliance audit.

- 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

To support ongoing accountability and transparency, you should publicly report these annual statistics to inform the public about your program and strengthen public confidence that facial recognition technology is being used responsibly.

Recommendations:

17.1 Set and follow ongoing accountability measures, including annual compliance audits, to assess your 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 your 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 your program.

Appendices

Appendix A: Key Recommendations

Below are key recommendations, for reference purposes only.

When designing and using a facial recognition mugshot database program in Ontario, the IPC recommends police services boards and police services:

Key consideration 1: lawful authority and lawful operation

1.1 Ensure you have lawful authority to operate a facial recognition mugshot database program and your authority is clearly documented before you start the program. If you are already operating a program, re-evaluate lawful authority as soon as possible.

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

1.3 If there are any gaps in lawful authority, legal compliance, or rights protections, you should adjust the scope of the FR mugshot database program to ensure compliance with the law and the protection of fundamental rights.

Key consideration 2: guiding principles

2.1 Draft and publicly communicate a statement of guiding principles for the use of FR in connection with mugshot databases 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 a facial recognition mugshot database program.

Key consideration 3: mugshot databases and related policies

3.1 Before putting in place an FR mugshot database program, review arrest record policies and retention schedules, particularly those governing mugshot databases, to ensure they do not permit or facilitate the excessive, discriminatory, unconstitutional, or otherwise unlawful retention and use of mugshot records.

3.2 Before putting in place an FR mugshot database program, and on an annual basis moving forward, purge mugshot databases of records that reflect or may facilitate excessive, discriminatory, or unlawful police practices, including by purging:

- non-conviction arrest records
- arrest records tied to summary offences, including hybrid offences after the Crown has elected to proceed on a summary basis and
- arrest records of persons dealt with under the *Youth Criminal Justice Act* (YCJA), after the YCJA access periods have expired

3.3 If you are currently operating an FR mugshot database program, review and purge mugshot records consistent with recommendations 3.1 and 3.2, starting as soon as reasonably practical but no later than one year following the release of this guidance and on at least an annual basis moving forward.

Key consideration 4: privacy impact assessments

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

4.2 Your PIA report should identify and address the privacy risks of using facial recognition technology in the mugshot database context (e.g., as described above) and include safeguards and controls that can be built into the program's policies and procedures to mitigate these risks.

4.3 Share the results of your PIA with your police services board and make the PIA report, or a summary of it, 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 your PIA.

Key consideration 5: scope, purpose, and program policies

5.1 Establish and limit the scope and purpose of your FR mugshot database program from the beginning, by focusing on generating investigative leads for the purpose of identifying individuals reasonably suspected of having committed a serious offence. Ensure the scope and purpose are maintained over time and comply with applicable law and the privacy principles of reasonableness, necessity, and proportionality.

5.2 Develop and approve comprehensive policies and procedures for your FR mugshot database program consistent with the recommendations in this guidance.

Key consideration 6: public engagement

6.1 Conduct meaningful public consultations with affected communities and interested parties about your program before putting it in place. In the case of current or ongoing programs, public consultations should still occur.

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

Key consideration 7: transparency

7.1 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 to foster ongoing transparency.

This public information should include:

- 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 your 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 facial recognition 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
- information about how individuals can request access to and correction of their personal information

Key consideration 8: pilot programs

8.1 Conduct a time-limited pilot program with clear goals and objectives before fully implementing the 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.

Key consideration 9: quality of probe images

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

Key consideration 10: retention of probe images

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. These should be consistent with the circumstances described in this guidance.

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

Key consideration 11: accuracy, human review and oversight of results

11.1 Take steps to test for bias and inaccuracy in the performance of the FR system as a whole, 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, for example to avoid false positives and support program evaluation.

11.2 Set and follow transparent procedures for the human review and accuracy controls of your 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 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.

Key consideration 12: limited collection, retention, use, or disclosure of personal information and reasonable safeguards

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 your 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 different parts of your 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.

Key consideration 13: access, correction, and expungement rights

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

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

Key consideration 14: requests from other police services

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 other police services to run FR searches in your 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, such as FR search requests received, whether they were processed and how, their results, and the information returned to the requesting police service, if any

Key consideration 15: joint facial recognition mugshot database programs

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 this 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 this 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, (e.g., it focuses on only generating investigative leads for serious crimes)
- 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 in relation to non-conviction arrest records set out in key consideration 3.

15.4 Each police services board involved should regularly audit and evaluate the effectiveness and appropriateness of any joint program and make audit reports and evaluations publicly available.

Key consideration 16: ongoing monitoring and reassessment

16.1 Once your 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 facial recognition technology.

16.2 Decide whether any existing risk assessments, program policies, procedures, or the overall design and operation of your program or FR system need to be re-evaluated and updated.

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

Key consideration 17: accountability

17.1 Set and follow ongoing accountability measures, including annual compliance audits, to assess your 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 your 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 your program.

Appendix B: Glossary

Biometric information: Biometric information is personal information resulting from specific technical processing relating to the physical characteristics of an individual, used to confirm identity.

Facial recognition technology: Facial recognition technology uses image processing software to detect and analyze the features of an individual's face to identify or verify an individual's identity. While early versions relied on humans to manually select and measure the landmarks of an individual's face, today, the process of creating a facial template or faceprint is fully automated by FR technology. Using advanced, deep learning algorithms trained on millions of examples, facial recognition technology creates three-dimensional faceprints consisting of close to a hundred biometric features from one or more two-dimensional images.

Facial recognition algorithms: Facial recognition works by performing a series of discrete tasks. There are four key tasks, each of which is automated using an algorithm. However, taken together, they form one overarching algorithm for the system. Their work may be described as follows:

- A *face detector* scans an image and picks out the faces in it.
- A *faceprint generator* takes an image of a face and creates a faceprint of it.
- A *faceprint comparator* compares two faceprints and returns a similarity score.
- A *faceprint matcher* searches a database of faces and (using the faceprint comparator) returns a list of candidates whose similarity score is at, or above a given threshold.

Faceprint: A faceprint is a template of the biometric features of a person's face. It contains a set of unique physical characteristics inherent to an individual that cannot be easily altered. Examples of biometric features encoded in a faceprint may include the distance between eyes, width of nose, shape of cheekbones and length of jaw line.

False positives: False positives are errors where the FR algorithm returns a candidate match in the database that is not of the individual in the probe image.

False negatives: False negatives are errors where the FR algorithm fails to return a genuine match in the database even though the database contains one.

Identification: Refers to determining the identity of an otherwise unknown individual. In the FR mugshot database program context, facial recognition compares a probe image against all other images in a database of pre-enrolled faces in an attempt to learn the individual's identity. This is sometimes referred to as "1: N" matching.

Non-conviction arrest record: A non-conviction arrest record is an arrest record where an individual was charged with a criminal offence if the charge was dismissed, withdrawn, or stayed, or resulted in a stay of proceedings or an acquittal.

Probe image: Facial recognition systems take as input one or more images of individuals whose identities they then try to discover or verify. This inputted image is known as a probe image. The way a probe image is entered into a facial recognition system for identification purposes may vary.

Serious crime: For the purposes of this guidance, serious crime means indictable offences or hybrid offences under a federal law such as the *Canadian Criminal Code*. This is consistent with the *Identification of Criminals Act*, which only permits the police to take mugshots of individuals:

- charged with an indictable or hybrid offence or subject to an appearance notice, undertaking, summons or order in relation to an indictable or hybrid offence
- charged with offences under the *Security of Information Act*
- apprehended under the *Extradition Act* or
- in lawful custody pursuant to section 83.3 of the *Criminal Code*

Indictable offences are the most serious offences under the *Criminal Code.* They include theft over $5,000, aggravated sexual assault, and murder. A hybrid offence is a crime where a Crown attorney can decide whether to proceed summarily or by indictment, depending on the seriousness of the facts alleged. Note that police are not empowered to take mugshots of individuals charged with offences that are purely summary in nature.

Similarity score: To express the different ways faces may be similar or different, facial recognition systems calculate a similarity score, also sometimes referred to as a confidence score. This is a numerical value representing the degree of similarity between two faceprints based on the biometric features encoded in them. A lower value indicates less similarity, a higher value more.

Threshold: Even though two faceprints may have a positive similarity score, only those that meet or exceed a given threshold (e.g., a specific similarity score or a predetermined number of potential matches) are considered potential matches. Some facial recognition products allow the end user to set the threshold; others do not. How the threshold is set directly affects the number of results returned

in a given search, with implications for the accuracy, including error rates, of the algorithm. Depending on the circumstances, some implementations may require higher thresholds than others.

Training data: The image processing algorithms that power FR are generated using machine learning methods that require a large number of labelled examples of individuals' faces for training. This set of labelled examples is known as the training data of the algorithm.

Facial Recognition and Mugshot Databases: Guidance for Police in Ontario

2 Bloor Street East,
Suite 1400
Toronto, Ontario
Canada M4W 1A8

www.ipc.on.ca
416-326-3333
info@ipc.on.ca

January 2024