Information and Privacy
Commissioner of Ontario
Commissaire à l'information et à la
protection de la vie privée de l'Ontario

January 10, 2024 ***VIA ELECTRONIC MAIL & ONLINE SUBMISSION***

Ann Morgan
Chair
Toronto Police Services Board
40 College Street
Toronto, ON M5G 2J3

Dear Ms. Morgan:

RE: *Update on the Implementation of the Board's Policy on Use of Artificial Intelligence Technology* in relation to the facial recognition mugshot database program and other AI technologies used by the Toronto Police Service

I am writing to provide the Toronto Police Services Board (the Board) with the submission of the Information and Privacy Commissioner of Ontario (the IPC) regarding a report entitled, *Update on the Implementation of the Board's Policy on Use of Artificial Intelligence Technology* (the Report) scheduled to be discussed at the Board's public meeting of January 11, 2024. In the interest of transparency to the public, I will be posting this letter to the IPC's website.

The Report describes five artificial intelligence systems currently in use by the Toronto Police Service (the Service). The Report indicates that the Service has assessed one of those technologies as *high risk* under the Board's *Policy on Use of Artificial Intelligence Technology* (the Policy). That *high-risk* technology involves the use of facial recognition to search the Service's mugshot database.

The present deputation focuses primarily on the Board's consideration of the Service's facial recognition mugshot database program. I am particularly concerned that the Board may conclude its review of the Service's facial recognition mugshot database program as early as January 11, without the benefit of the IPC's soon to be released *Facial Recognition and Mugshot Databases: Guidance for Police in Ontario* (the *Guidance*).

The IPC has been consulting interested parties on its *Guidance* for months. My office shared a draft version with the Service and the Board in the spring of 2023 and received detailed written comments, many of which were very helpful and have since been thoughtfully considered and integrated. In our view, the *Guidance* benefited substantially from the input of all those who participated in the *Guidance* consultation, including senior staff of the Service and the Board.

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

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel/Tél : (416) 326-3333
1 (800) 387-0073
TTY/ATS : (416) 325-7539
Web : www.ipc.on.ca

In view of the speed with which the Board appears to be moving, I have decided to provide the Board with an advance copy of the text of the final *Guidance* (attached). The IPC will be formally publishing the *Guidance* in English and French in the coming weeks. You will see that the *Guidance* provides Ontario police services boards and police services - including those already operating facial recognition mugshot database programs - with a comprehensive set of recommendations designed "to help reduce specific risks associated with facial recognition mugshot database programs." These recommendations include:

- commit to reviewing your current program against this guidance as soon as possible,
- ensure that the design and operation of your programs, including use of any third-party service providers, meet all legal requirements and include rigorous privacy and transparency safeguards and controls,
- conduct a comprehensive privacy impact assessment (PIA), make the PIA report - or a summary of it - publicly available, and conduct other risk assessments such as security, human rights, and algorithmic impact assessments as needed, and ensure these are combined or coordinated with your PIAs, conduct meaningful public consultations with affected communities and ensure they consider the privacy and equity concerns of marginalized communities, including those who are disproportionately affected by systemic discrimination and over-policing practices,
- limit the purpose of your facial recognition 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, and ensure this purpose is maintained over time and complies with applicable law and the privacy principles of reasonableness, necessity, and proportionality,
- before putting in place a facial recognition mugshot database program, and on an annual basis thereafter, review your arrest record policies and retention schedules, and purge your mugshot database(s) of records that reflect or may facilitate excessive, discriminatory, or unlawful police practices,
- set and follow clear standards for ensuring minimum photo quality of probe images, clear rules and processes for their retention and secure destruction, and appropriate oversight mechanisms for regularly confirming compliance,
- take steps to test for bias and inaccuracy in the performance of the FR system as a whole, set and follow transparent procedures for human review and accuracy controls, and document all assessment results,
- ensure you have clear and publicly available policies and procedures on access, correction, and expungement rights, and
- post up-to-date, readily available, plain language information about your program on the websites of both the police services board and the police service to foster ongoing transparency.

The IPC urges the Board and the Service to consider and follow the IPC's *Guidance* before you conclude your review of Toronto's facial recognition mugshot database program under the Policy. In addition, we note that the Ontario Human Rights

Commission's (OHRC) December 14, 2023 report, *From Impact to Action*, the final report on its inquiry into anti-Black racism by the Toronto Police Service (*From Impact to Action*) contains several relevant findings and recommendations that the Board ought to also carefully consider.

In particular, the OHRC report confirms that Black people are charged at a disproportionately higher rate, overrepresented in cases that resulted in a withdrawal of charges, and their cases are less likely to result in a conviction compared to cases involving White people. Moreover, the report indicates that "68% of charges were stayed or withdrawn in Ontario in 2018–19, which indicates broad patterns of over-charging that result in courts being flooded with cases that are very unlikely to result in convictions." Recalling that, as of May 2019, the Service's mugshot database contained approximately 1.5 million mugshots, it is conceivable that tens or even hundreds of thousands of the mugshots retained by the Service may be associated with individuals who have *never been convicted of a criminal offence and face no outstanding criminal charges*. In this context, the IPC agrees with the OHRC's recommendations that the Service should:

- limit the use of AI technologies until privacy and human rights assessments are conducted, and the OHRC, IPC and experts in technological/algorithmic racial bias are consulted, and
- purge its database of photographs, fingerprints or other biometric information from charges that do not result in convictions (for example, the IPC suggests doing so, once a reasonably short defined period – such as one year – has elapsed following a final disposition).

The IPC believes that its *Guidance* and the OHRC's *From Impact to Action* report will assist both the Board and the Service as you continue the vital work of identifying and mitigating the privacy and human rights risks associated with your facial recognition mugshot database program. Taking the time necessary to complete this work would be consistent with Chief Demkiw's September 5, 2023, acknowledgement that the Service's "use of facial recognition software, while a valuable tool for investigators, raises concerns from community members in relation to improper use and surveillance". It would also allow time for the Service to complete the audits discussed by the Chief in his September 2023 *Annual Audit Report* with respect to the Service's facial recognition mugshot database controls and the Service's policies and processes for the destruction of adult fingerprints, photographs and records of dispositions associated with non-conviction dispositions.

Additional concerns

The Report under consideration also discusses four other artificial intelligence or AI technologies currently being used by the Service and designates these as *low risk* technologies. In our respectful view, none of these technologies can reasonably be described as *low risk* under the Board's own Policy. At a minimum, consider that:

1. the Service's use of an automated fingerprint identification system (AFIS), two automated license plate recognition systems (one for police vehicles, and one for parking enforcement, including to identify stolen vehicles), as well as the BriefCam "could be used to assist in the identification of individuals for the purpose of their arrest, detention or questioning", and
2. the Service's use of AFIS appears to amount to "an application which links biometrics to personal information."

Both these factors are consistent with the definition of a *high-risk technology*, as per the Board's Policy. In this context, we recommend that:

- the Board direct the Service to either re-designate these four AI technologies as high risk and proceed to comply with the mitigation related requirements of the Policy (per section 19) or re-evaluate them under the Policy, before reporting back to the Board (per section 16).

Lastly, we note that the Board is amending the definition of artificial intelligence technology to exclude technologies which require a privacy impact assessment but are not ultimately determined to involve the use of "AI as it is generally understood." On this last point, we offer the following recommendations:

- in making determinations as to whether privacy-impacting technologies or programs include (or do not include) the use of artificial intelligence, the Service should be thorough and rigorous in its evaluation and documentation of how it reached its decisions,
- with the rapid adoption of artificial intelligence in software development, an existing technology can quickly and easily evolve to include AI functionality, potentially without the full knowledge of its users. On that basis, we recommend the regular evaluation of <u>all</u> privacy-impacting technologies to ensure that those that were originally deemed "non-AI" have not since adopted AI functionality that would require further assessment under the Policy, and
- whether privacy-impacting technologies used by police engage AI functionality or not, it is a best privacy and transparency practice to make details of the technology available to the public, in support of preserving and promoting public accountability and trust in law enforcement.

In light of all of the above, our overarching recommendation to the Board is that it and the Service commit to taking the additional time necessary to carefully assess and mitigate the privacy and human rights risks associated with all five of the artificial intelligence systems currently in use by the Service.

The Board, the Service, the OHRC, and my office, have had a strong track record of communicating openly and working cooperatively to help achieve transparent and accountable service delivery designed to protect the privacy and human rights of Ontarians. I remain committed to that approach here and welcome further consultation and engagement in the weeks and months ahead.

Sincerely,

Patricia Kosseim
Commissioner

CC: Myron Demkiw, Chief

Enclosure