Toronto Police Accountability Coalition

www.tpac.ca, info@tpac.ca

 December 4, 2021.

To Toronto Police Services Board

Artificial Intelligence programs for police raise a number of critical issues which need to be addressed.

They are costly to purchase, to train officers, and costly to operate. While police services will state that AI will help save police money, given past performance it is very unlikely that police budgets will be reduced to reflect any such savings.

The programs are not helpful in addressing the violence which affects too many people – violence in the home and sexual assault. They do not help people be safe and secure.

The programs are not about prevention, but function in an after-the-fact way, perhaps helping to identify perpetrators. Predictive policing is apparently about prevention, but it is highly discriminatory.

AI discriminates against a number of groups of people, and to that extent can cause much harm.

Policing seems to have been caught up in the belief that more technology such as cameras, conducted energy weapons, and AI will make policing more effective, but policing never seems to reach that goal, and the powerful policing culture seems to always win out over any positive changes which people want to make.

For these reasons, one should be very skeptical about the use of AI in policing. Our brief is presented with the understanding that if a decision is made to proceed with AI, it should be done only on the basis of the policy outlined below.

A few notes of methodology

1. Everything underlined is new; the rest is all taken from the TPSB draft.

2. The TPSB draft contains so many sub-clauses that it is difficult to know what is being proposed. Our draft limits the number of sub-clauses to make it much easier to understand.

3. The idea of classifying the risks has been deleted. It is more accurate to proceed on the assumption that all AI is risky. Certainly, programs such as Google Translate involve a minimum risk, but this can be flagged in the impact assessment.

4. Many ideas from the Citizen Lab report `To Surveil and Predict’ have been incorporated. That report is very helpful.

5. The idea of prohibiting in principle the use of biometrics – facial, gait and voice recognition – is taken from the draft policy for the European Union.

Proposed policy

1. It is recognized that there are three broad categories of AI technologies: those that are location based, which attempt to predict where crime will occur; those that are person-focused, which attempt to predict who will be involved in criminal activity; those involving surveillance, which collect and process general amounts of data. Surveillance technologies include automatic license plate readers; social media surveillance; facial recognition; social network analysis. All such technologies generalize data and stereotype that data in ways which discriminate against different groups of individuals and are prone to systemic racism, and for that reason are unreliable and must be subject to very powerful sanctions before they can be considered for use. Technologies may change in the future in ways which minimize discrimination, and when that happens it will be made clear in the impact assessment undertaken.

2. The Service will develop, in consultation with experts and stakeholders who are independent of police including the Information and Privacy Commissioner of Ontario, the Ministry of the Attorney General and other stakeholders, independent human rights, legal and technology experts and affected communities, procedures and processes for the review and impact assessment of new AI technologies. Police will provide reasonable funding to non-government groups for such independent consultations.

3. The impact assessment of new AI technologies will include, at a minimum, answers to the following questions: is the technology reliable; is the technology appropriate to the tasks and objectives given the costs, risks and harms; are their reasonable alternatives to the use of the technology; possible unintended consequences of the proposed use of the AI technology, including possible effects on procedural fairness, due process, gender and race equality, or disproportionate impacts on *Human Rights Code* protected groups; and any approval requirements for any new AI technology.

The impact assessment will also include: where applicable, a legal analysis of potential challenges to the admissibility of evidence generated or impacted by the AI technology in criminal proceedings; the findings of any risk analyses that have been done, including any analyses required by the Information and Privacy Commissioner of Ontario; any reports and documentation used in the evaluation of AI technology; a mitigation plan to mitigate the risks posed by the implementation of the AI technology; the estimated cost of acquiring and implementing the AI technology, and any additional costs or savings expected from the implementation of the AI technology; and, proposed indicators that will be used to tracked its use until at least 12 months after full deployment of the new AI technology to determine whether the AI technology is achieving its intended goal and whether its deployment has had any unintended consequences;

4. All technologies must undergo the impact assessment defined above before they are employed by the Service, and such assessments must be approved by the Board prior to any use by the Service, and the Board must approve any conditions recommended by the independent assessment to be applied to the use of any AI technology.

5. All expenditures for AI technology must be approved by the Board.

6. Service Members may not use new AI technologies prior to receiving approval in accordance with the procedures and processes established pursuant to this policy.

7. All Service Members must be trained in new AI technologies prior to receiving approval to use such technologies. Training must also include ethical issues involved in using AI.

8. The accuracy of all personal information must first by verified by a defined individual before it is stored in a data base.

9. Members of the public have the right to have information stored in the data base concerning them destroyed, and processes will be established to permit this to occur.

10. Because AI technologies always include acknowledged or unforeseen biases, AI technologies are prohibited from being used to stop, detain, or arrest individuals.

11. The live use of biometric identification systems including facial, gait and voice recognition, is prohibited in principle. Only after judicial approval may it be used in exceptional circumstances such as to look for a missing child, to prevent a specific and imminent terrorist threat, or to detect, locate and identify a suspect of a serious criminal offence.

12. Judicial approval is required before historical data may be used in AI technology and before AI technology is used at public gatherings or for on-line surveillance.

13. AI technology may only be used only in accordance with applicable privacy laws, the *Human Rights Code* and the *Charter of Rights and Freedoms* and other legislative and legal requirements, including training, and governance structures.

14. Data created for the intent of supporting AI, and created by and emanating from the use of AI technology, will not be shared with another government agency or with the private sector unless the Board has approved such sharing, and the Board will exhibit extreme caution in approving such sharing.

15. Certain AI Technologies may not be considered for adoption by the Service or the Board where they include:

1. Any application where there is no “human-in-the-loop”. A human must recognize that AI results are not `truth’ but only recommendations, and that person must evaluate a recommendation from an AI tool before consequential action is taken;
2. Where use of the application results in mass surveillance defined as the indiscriminate covert monitoring of a population or a significant component of a population;
3. Any application of AI in a life-safety situation, i.e., an application where the action of the AI technology could slow down the reaction time of the human operator, resulting in potential risk to life of members of the public or Service Members;
4. Any application known or is likely to cause harm or have an impact on an individual’s rights, despite the use of mitigation techniques, due to bias or other flaws; or
5. Where training or transactional data is known or thought to be illegally sourced or where it is from an unknown source;
6. Where training or transactional data is known to be of poor quality, carry bias, or where the quality of such data is unknown;
7. Where training data can be influenced or biased by malicious actors;
8. Applications which link biometrics to personal information (e.g. facial recognition); or
9. Where a system cannot be fully explainable in its behaviour;
10. Where the “human-in-the-loop” may have difficulty identifying bias or other decision iii. for a purpose or in a manner not previously approved by the Board.

16. It is the policy of the Board that the Chief of Police will monitor from the initiation of deployment and until 12 months after full deployment of the new AI technology is approved by the Board, and that advice will be sought from an independent expert regarding such deployment.

17. The Chief will report to the Board, within 15 months of full deployment of a new AI technology, and include in such report the advice of an independent expert. This report will include:

(a)  How the AI technology has generally been deployed or utilized within the first period until 12 months from full deployment, including with respect to compliance with applicable privacy laws and other legislative and legal requirements;

b)  The performance as measured by the indicators approved by the Board;

(c)  What concerns the Chief of Police has seen raised by members of the public or Service Members, and how the Chief has acted to address those concerns;

(d) Whether the Chief intends to continue using the AI technology in the same manner or in a different manner in the future; and

18. It is also the policy of the Board that the Service will provide a user friendly explanation of the AI system of approval and use to ensure maximum transparency, and provide a framework for easy access to information regarding AI technologies used by the Service.

19. The Executive Director shall create a method for members of the public to submit concerns pertaining to AI technologies used by the Service through the Board’s website. Where a communication from a member of the public amounts to a complaint, will advise the individual of their right to file a complaint with the Board, the Office of the Independent Police Review Director or successor role, or forward the communication to the Chief of Police, as appropriate, and inform the complainant of this action. The Board will review the reports of the Executive Director and determine whether the Service may continue to use the AI technology in question, and whether any additional analysis, monitoring, auditing and reporting requirements are to be imposed.

20. The Chief of Police will post on the Service’s web site no later than December 2024, and maintain up to date, a list of all AI technologies currently in use by the Service, including the following information:

1. Name and manufacturer/developer,
2. Purpose of the technology,
3. How the technology is used by the Service,
4. What information is collected by the technology, and
5. What persons or under what circumstances can the technology be expected to be used;

21. The Service will report to the Board and terminate the use, immediately upon identification, and no later than December 2024, of any AI technology in use by the Service prior to the adoption of this Policy, which has not been approved by the Board.

22. On a report from the Chief, the Board will review at least once every five years the use of any AI technology to ensure that the AI technology has not been put to use for a novel purpose or in novel circumstances that may substantially change the data collected or used, in a manner that would constitute a new AI technology, or the risk level of the AI technology, and, where it is found that an AI technology has been put to a new use in this manner, will report to the Board as soon as possible, in accordance with section 5.