Dr. Dubi Kanengisser
Senior Advisor, Strategic Analysis and Governance
Toronto Police Services Board
dubi.kanengisser@tpsb.ca

[*delivered electronically*]

December 15, 2021

Dear Dr. Kanengisser:

**Re: Submission to the Toronto Police Services Board's Use of New Artificial Intelligence Technologies Policy**

We write to you as a group of experts[1] in the legal regulation of artificial intelligence (AI), technology-facilitated violence, equality, and the use of AI systems by law enforcement in Canada. We have experience working within academia and legal practice, and are affiliated with LEAF and the Citizen Lab who support this letter.

## About LEAF

The Women's Legal Education and Action Fund (LEAF) is a national, charitable, non-profit organization that advances substantive gender equality through litigation, law reform, and public education. LEAF and its Technology-Facilitated Violence Advisory Committee have developed expertise on issues related to technology and equality. In 2019, LEAF intervened in the Supreme Court of Canada case, *R v Jarvis*[2], where it urged the Court to apply an equality-focused lens when interpreting the *Criminal Code* provision of voyeurism. In 2019, it a made submissions to Parliament

[1] Kristen Thomasen (co-author and signatory; Assistant Professor, Peter A. Allard School of Law, University of British Columbia); Suzie Dunn (co-author and signatory; Member of LEAF's Technology-Facilitated Violence Advisory Committee; Assistant Professor, Dalhousie University's Schulich School of Law); Kate Robertson (co-author and signatory; Research Fellow, Citizen Lab; criminal and regulatory litigator, Markson Law); Pam Hrick (reviewer and signatory; Executive Director & General Counsel, Women's Legal Education and Action Fund); Cynthia Khoo (reviewer and signatory; Research Fellow, Citizen Lab); Rosel Kim (reviewer and signatory; Staff Lawyer, Women's Legal Education and Action Fund); Ngozi Okidegbe (reviewer and signatory; Member of LEAF's Technology-Facilitated Violence Advisory Committee; Assistant Professor of Law at Cardozo School of Law); and Christopher Parsons (reviewer and signatory; Senior Research Associate, Citizen Lab).
[2] 2019 SCC 10.

on a study on online hate.[3] In 2021, it released a report on an equality-centred approach to content moderation, titled "Deplatforming Misogyny".[4] LEAF also made submissions to Canadian Heritage on the Federal Government's Proposed Approaches to Address Harmful Content Online.[5]

## About Citizen Lab

The Citizen Lab at the Munk School of Global Affairs & Public Policy, University of Toronto ("Citizen Lab"), is an interdisciplinary laboratory which focuses on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security. We use a "mixed methods" approach to research combining practices from political science, law, computer science, and area studies. Our research includes: investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

Citizen Lab has conducted in-depth analysis of the human rights impacts of emerging technologies in the areas of predictive policing and algorithmic surveillance. Its findings and law reform recommendations are found in a report that was released in 2020 by the Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto) and the International Human Rights Program (University of Toronto's Faculty of Law), titled *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada* (*"To Surveil and Predict"*).[6] The co-authors of this submission who are affiliated with the Citizen Lab are submitting this letter and recommendations that emerge from the aforementioned report in their individual capacities as Citizen Lab researchers.

## Introduction

We commend the Toronto Police Services Board (TPSB) for engaging in this public consultation and welcome this opportunity to submit comments on the TPSB's Use of Artificial Intelligence Technologies Policy (AI Policy). In this submission, we urge the TPSB to **centre precaution, substantive equality, human rights, privacy protections, transparency, and accountability** in its policy on the use of AI technology by the Toronto Police Services (TPS). Further, we implore the Board to continue to seek out the guidance and expertise of AI and technology scholars and advocates; equality and human rights experts; affected communities and

[3] Women's Legal Education and Action Fund, "Submission to the House of Commons Standing Committee on Justice and Human Rights Respecting the Committee's Study of Online Hate" (2019), online (pdf): Women's Legal Education and Action Fund <https://www.leaf.ca/wp-content/uploads/2019/05/2019-05-10-LEAF-Submission-to-the-Standing-Committee-on-Justice-and-Huma....pdf>.

[4] Cynthia Khoo, "Deplatforming Misogyny" (April 2021), online (pdf): Women's Legal Education and Action Fund <https://www.leaf.ca/publication/deplatforming-misogyny/>.

[5] Moira Aikenhead, Suzie Dunn, & Rosel Kim, "Canadian Heritage on the Federal Government's Proposed Approaches to Address Harmful Content Online" (25 September 2021), online (pdf): Women's Legal Education and Action Fund <https://www.leaf.ca/submission/leaf-submission-to-canadian-heritage-on-online-hate/>.

[6] Kate Robertson, Cynthia Khoo, & Yolanda Song, "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada" (September 2020), Citizen Lab and International Human Rights Program, University of Toronto, online: <https://citizenlab.ca/2020/09/to-surveil-and-predict-a-human-rights-analysis-of-algorithmic-policing-in-canada/>.

their members, including historically marginalized communities; and other relevant stakeholders when developing and implementing policies related to the adoption and use of AI by the TPS today, and into the future. Finally, we recommend that the TPSB place an immediate moratorium on law enforcement use of algorithmic policing technologies that do not meet minimum prerequisite conditions of reliability, necessity, and proportionality.[7] We appreciate and recognize that our comments will be shared publicly.

We have reviewed the draft policy and provide comments and recommendations focused on the following key observations:

1. Police use of AI technologies must not be seen as inevitable
2. A commitment to protecting equality and human rights must be integrated more thoroughly throughout the TPSB policy and its AI analysis procedures
3. Inequality is embedded in AI as a system in ways that cannot be mitigated through a policy only dealing with use
4. Having more accurate AI systems does not mitigate inequality
5. The TPSB must not engage in unnecessary or disproportionate mass collection and analysis of data
6. TPSB's AI policy should provide concrete guidance on the proactive identification and classification of risk
7. TPSB's AI policy must ensure expertise in independent vetting, risk analysis, and human rights impact analysis
8. The TPSB should be aware of assessment challenges that can arise when an AI system is developed by a private enterprise
9. The TPSB must apply the draft policy to all existing AI technologies that are used by, or presently accessible to, the Toronto Police Service

## Background

When police forces employ AI-based technologies, there can be considerable risk to the protected rights of individuals and communities. Any decision by the TPSB to authorize TPS use of AI systems that risk the equality, privacy, dignity, and human rights of individuals must be made with caution, transparency, accountability, and explicit consideration of its potential impact on human rights. For the purpose of this submission, we focus on AI systems that put these rights at risk. We are not directly concentrating on low-risk technologies that have no potential to impact on these human rights-protected interests, such as seemingly mundane forms of software like a grammar editing software that utilizes AI.

As noted in the Citizen Lab's report, *To Surveil and Predict*,[8] algorithmic policing "has the potential to violate fundamental human rights and freedoms that are protected under the *Canadian Charter of Rights and Freedoms* ('the *Charter*') and international human rights law...[especially]… the right to privacy; the right to freedoms of expression, peaceful assembly, and association; the right to equality and freedom from discrimination; the right to liberty and to be free from arbitrary detention; the right to due process; and the right to a remedy."[9] These known and potential

[7] Robertson, Khoo, & Song, *To Surveil and Predict*, *supra* at p. 5, 150-151, 154-155.
[8] *Ibid.*
[9] *Ibid* at 3.

violations must be avoided at all costs. It is critical that the use of potentially rights affecting AI by the TPS not be considered inevitable.

For these reasons, the development of a policy for the use of AI by the TPS is important. As the first police service in Canada to initiate such a policy, it is crucial that the TPSB develop a robust and well-informed set of guidelines, as these guidelines may influence the subsequent development of policies across the country. For this reason, we commend this public consultation and hope the TPSB will give appropriate weight to the public submissions and ensure that its guidelines protect substantive equality and human rights.

There are many reasons why AI systems may seem appealing to police forces. AI may appear to hold the promise of improving the efficiency and accuracy of policing while reducing cost. However, this promise must be viewed with an eye to caution. AI systems are not consistently the neutral, effective, or necessary technologies they are often framed to be. Many algorithmic policing systems have been proven to replicate and even amplify discriminatory and racial bias, impacting the equality rights of protected groups, many of whom already face unacceptable rates of discrimination in the criminal justice system.[10] For example, facial recognition technology has been proven to be less accurate in the identification of Black faces, which has already led to wrongful arrests.[11] Even a perfectly accurate AI system, though, could amplify discriminatory bias and cause harm, such as perfecting mass data collection, analysis, and storage, including for biometric recognition systems, which heighten the risk of mass surveillance by the state. In other cases, such as in the case of Clearview AI,[12] the underlying data that an AI-driven software system relies upon may be collected in illegal or unethical ways that violate people's privacy rights.

Importantly, we also caution that the vulnerability of equality-seeking groups must not be coopted inappropriately in order to secure support for the broader use of AI systems by law enforcement. At times, the alleged protection of vulnerable groups, such as women and children, from exploitation, violence, and victimization have been employed to validate increased police powers and new investigatory techniques.[13] Additionally, the sanctioned use of an AI-system for one discreet purpose must not be assumed to validate its use in other contexts, or at all. The TPSB must be alert to scope creep when evaluating the use of AI-enabled systems by the Toronto police force.

---

[10] See e.g. Kristian Lum & William Isaac, "To Predict and Serve" (2016) 13:5 Significance 14; Joy Buolamwini & Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification" (2018) 81 Proceedings of Machine Learning Research 1.

[11] Kashmir Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match" *New York Times* (29 December 2020); Miriam Marini, "Farmington Hills man sues Detroit police after facial recognition wrongly identifies him" (April 13, 2021) Detroit Free Press, online: https://www.freep.com/story/news/local/michigan/2021/04/13/detroit-police-wrongful-arrest-faulty-facial-recognition/7207135002/.

[12] PIPEDA Finding #2021-001, "Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta", (2 February 2021) Office of the Privacy Commissioner, online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/>.

[13] See e.g. Corinne Mason & Shoshana Magnet, "Surveillance Studies and Violence Against Women" (2012) 10 Surveillance & Society 105 at 114-116; Kristen Thomasen, "Beyond Airspace Safety: A Feminist Perspective on Drone Privacy Regulation" (2016) 16 Canadian Journal of Law and Technology 307 at 324-328.

## Comments on the Draft Policy from a Substantive Equality Perspective

### 1. Police use of AI technologies must not be seen as inevitable

We appreciate TPSB's explicit recognition that some automated technologies carry so much risk that they should not ever be deployed in law enforcement contexts (policy s. 3). However, we also urge TPSB to strengthen its proposed limits on the use of AI systems.

TPS and TPSB must resist adopting systems which are marketed as having law enforcement promise but which lack strong evidence that the technologies will not replicate or entrench inequality or violate other rights. For example, as written now, the draft policy does not impose an obligation to treat the absence of independent validation of a technology as a high-risk factor. As will be discussed further in this submission, this gap leaves it open to the TPS to assess the risk of a technology based on a private companies' marketing materials that offer "evidence" of the tool's utility or purported absence of risk. By way of further example, the policy currently lists facial recognition systems as an example of a High Risk Technology, meaning such systems could be used with oversight, yet numerous facial recognition systems have already been shown to replicate and entrench inequality.[14]

The TPSB must also immediately assess existing AI systems used by the TPS to examine it for potential bias and consider its continued use. For example, on the TPSB website's overview of the public consultation, it lists "speech-to-text transcription software to transcribe body-worn camera recording audio" as low risk.[15] However, these systems can misquote people who speak in vernacular English, particularly where that vernacular originates from racially marginalized communities, which may have a negative impact on evidence collected about their interactions with the TPS.[16]

Further, we refer TPSB to the recommendation in *To Surveil and Predict* concerning a moratorium on law enforcement use of algorithmic policing technologies that do not meet minimum prerequisite conditions of reliability, necessity, and proportionality.[17] These requirements are exceed the current risk categories that are outlined in the TPSB's consultation. The policy should recognize that some technologies must be barred on ground that they risk infringing upon constitutional or human rights, despite also potentially enhancing some policing capacities. We urge TPSB to operate from a precautionary approach given the known potential for harms and documented rights violations associated with AI-driven policing systems. This policy should not be seen as inherently opening a door to more law enforcement use of AI systems.

TPSB should also strengthen and make more explicit the wording in the policy that enunciates these limits. Specifically:

---

[14] See for example the citations in footnote 10, above.
[15] https://tpsb.ca/ai
[16] Allison Koenecke, Andrew Nam, Emily Lake, Joe Nudell, Minnie Quartey, Zion Mengesha, Connor Toups, John R Rickford, Dan Jurafsky, & Sharad Goel, "Racial Disparities in Automated Speech Recognition" (2020) 117:14 Proceedings of the National Academy of Sciences 7684. Online: <https://www.pnas.org/content/117/14/7684?utm_keyword=referral_input>
[17] Robertson, Khoo, & Song, *To Surveil and Predict*, *supra* at 154.

- s 1(a) should be revised from stating that "Service Members may not use new AI" to stating "Service members shall not use new AI";
- s. 1(c)(i) should be revised from a statement that certain extreme risk systems "*may* not be considered" to one stipulating that they "*will* not be considered"; and
- s. 1(c)(i)(2) should be revised from "mass surveillance defined as the indiscriminate *covert* monitoring" to "mass surveillance defined as the discriminate or indiscriminate monitoring".

Such clear and firm wording in the policy would reflect the recognition that there must be limits on the use of AI systems by the TPS.

While the intention of this policy seems to acknowledge the need for limits, and for ongoing assessment of AI-driven systems, we suggest it would be helpful to use more cautious language and to explicitly recognize that this policy is but one of many necessary measures to ensure safety and accountability in the use (where necessary) of AI systems by TPS. For instance, the phrasing that "This Policy will ***ensure*** the thoughtful consideration of the benefits and risks of obtaining and deploying any new technology using AI" (emphasis added, p 2) should be scaled back to recognize the possibility that not all risks and benefits will be recognized in the early adoption of an AI-system. We appreciate the ways in which the policy mandates ongoing oversight of the use of new technologies, though we raise further comments on the review process in subsequent sections of this letter.

**Recommendations:**

**Recommendation 1:**

**We recommend that** any policies used by TPSB to govern the TPS' procurement or use of AI-based technologies include a requirement that all AI-systems must meet the minimum prerequisites of reliability, necessity, and proportionality.

**Recommendation 2:**

**We recommend that** whenever a proposed or currently used AI-system cannot meet the prerequisites of reliability, necessity, and proportionality that the technology or system should either be banned or severely limited in its uses.

**Recommendation 3:**

**We recommend that** there be clear language in the policy that allows for the outright rejection of certain AI systems and a requirement to reverse course on a technology that is already in use if it is later found to violate the prerequisites of reliability, necessity, and proportionality.

## 2. A commitment to protecting equality and human rights must be integrated more thoroughly throughout the TPSB policy and its AI analysis procedures

We appreciate that the policy proposal recognizes the need to protect equality and human rights, as noted in the "Purpose of the Policy." In order to more fulsomely reflect this commitment,

the policy should also include specific language that stipulates that all reviews and assessments of AI systems will include an explicit consideration of *individual* rights, including equality, privacy, due process rights, and human rights. Reviews should also explicitly consider the risk that a technology may establish or reify *systemic* harms that are associated with these individual rights.

For example, in concrete terms, we recommend that the reference in paragraph (h) on page 7 to "gender and race equality" also include reference to socioeconomic inequality, to accompany the protected grounds under the *Human Rights Code* and in s. 15 of the *Charter*.[18] We make this recommendation because differential treatment of individuals and groups based on socioeconomic differences or other grounds of discrimination may follow should police services rely on data-driven patterns and inferences where communities have historically been subject to over-policing. The reliance by many AI policing systems on historical data risks causing systematic and disproportionate disadvantage to groups protected under the *Charter* and *Human Rights Code*.[19] Further, individuals who lack high-income socio-economic status must be given equally meaningful protection of their rights in Canada.

**Recommendations:**

**Recommendation 4:**

**We recommend that** under s. 5(g) of the policy, reporting to the TPSB include the identification of potential individual and systemic human rights violations and harms.

**Recommendation 5:**

**We recommend that** under s. 5(h) of the policy, reporting to the TPSB include the identification of any potential human rights violations that could be caused by an AI system on an individual level as well as the identification of any potential systemic harms that could be caused or replicated by the use of an AI system (e.g. crime prediction systems).

**Recommendation 6:**

**We recommend that** when conducting the risk analysis for the AI categorization that the policy explicitly state that it will consider the privacy, equality, and human rights on an individual and systemic level. Such language might be included under s 1(c)(i)(4)).

**Recommendation 7:**

**We recommend that** the word "socioeconomic" be added after the word "gender" in paragraph (h) on page 7.

## 3. Inequality is embedded in AI as a system in ways that cannot be mitigated through a policy only dealing with its use

[18] Race, national or ethnic origin, colour, religion, sex, age, mental or physical disability, sexual orientation, marital status, and citizenship.
[19] Robertson, Khoo, & Song, *To Surveil and Predict*, *supra* at p. 113-119.

We support the recognition in the policy of the ways in which automated technologies can perpetuate systemic bias, resulting in both individual and systemic discrimination (p 1). The recognition of systemic harm acknowledges the ways in which technologies can perpetuate social oppression, absent individual 'bad actors' who misuse the technology, and regardless of the potentially good intentions of individual law enforcement agents or agencies. We are also pleased to see the recognition in the draft policy that AI systems can and do replicate pre-existing bias and oppression (e.g p 3).

However, we are concerned that the policy does not acknowledge or address the ways in which inequality can be embedded in AI *as a system*,[20] and thus may be replicated by AI-driven tools employed in policing. The adoption of such an acknowledgement, alongside mitigation and prevention requirements, would align with policy requirement 5(h) to consider "unintended consequences" before a new AI-based tool is approved.

For example, the policy requires restraint in adopting systems that have been trained with unknown, illegal, or malicious data sets. The policy does not recognize or address the problems of bias and discrimination which may be latently embedded in some widely accepted datasets; such bias or discrimination would seemingly not be caught by the current provisions because this data is known and publicly available.[21] While the policy acknowledges systemic discrimination generally, it does not connect that with the design of AI systems themselves. For instance, the act of imposing categories or labels on training data can perpetuate inequality depending on how labels are used to sort, classify, identify, and analyze information about an individual, and thus to classify individuals – for example, where a system is trained on and replicates an inaccurate gender binary.[22] The policy does not pre-emptively mitigate the harm that is exerted by imposing a category *upon* someone, particularly in the high-stakes context of investigation or enforcement. We urge the TPSB to consider the ways in which the structure of an AI-system can itself perpetuate the bias that the "Purpose of the Policy" suggests TPSB intends to mitigate. We urge broader consideration of the potential harms of AI itself within the scope of all of the risk categories as well.

**Recommendations:**

**Recommendation 8:**

**We recommend that** TPSB explicitly acknowledge that limits on and oversight of AI system use is not itself enough to ensure TPS use of such systems will not engage constitutional and human rights. This recommendation is accompanied by the recommendations concerning vetting requirements that we discuss below in sections 6 and 7 as one mechanism for addressing some of the concerns raised here.

---

[20] Andrew Selbst, danah boyd, Sorelle Friedler, Suresh Venkatasubramanian, & Janet Vertesi, "Fairness and Abstraction in Sociotechnical Systems" FAT '19 Proceedings of the Conference on Fairness, Accountability, and Transparenty. Online: <https://dl.acm.org/doi/10.1145/3287560.3287598>

[21] see e.g. Buolamwini & Gebru, *supra*; Simone Browne, "Digital Epidermalization: Race, Identity and Biometrics" (2010) 36 Critical Sociology 131; Kate Crawford, *Atlas of AI* (Yale University Press: New Haven, 2021); and Amanda Levendowski, "How Copyright Law Can Fix Artificial Intelligence's Implicit Bias Problem" (2018) 93 Washington Law Review 579 on the bias issues in existing datasets.

[22] See e.g. Sasha Costanza-Chock, "Design Justice, AI, and Escape from the Matrix of Domination" (July 16, 2018) Journal of Design and Science, <https://jods.mitpress.mit.edu/pub/costanza-chock/release/4>.

## 4. Having more accurate AI systems does not mitigate inequality

While the proposed policy seeks to restrain the use of systems trained on unknown or potentially altered data, the alternative of having more accurate and vetted data and systems does not on its own make these systems safe or appropriate.

More accurate and pervasive surveillance or policing supported by AI is not necessarily better for all people, particularly those who are members of already over-policed communities. In fact, the use of AI risks inappropriately expanding police capabilities and bring marginalized people into greater contact with the police in ways that will replicate existing discriminatory practices in policing. In Canada, it is recognized that Indigenous, Black, racialized, low-income, and 2SLGBTQ+ people are over-policed and over-represented in the prison system.[23]

For example, as currently drafted, software systems that are used to assess or predict crime location with the goal of streamlining the deployment of officers could be categorized as potentially posing 'moderate' risks. However, such technologies can exacerbate pre-existing inequities, such as when the system is trained on historical policing data, replicating over-policing of specific neighbourhoods, regardless of whether that system can be said to be "accurate" or not.[24] Such systems should be classified as extreme risk.

**Recommendations:**

**Recommendation 9:**

**We recommend that** the policy include a required assessment of, and justification for, TPS collection and use of data to be processed through or otherwise utilized by algorithmic policing systems.

**Recommendation 10:**

**We recommend that** the policy recognize that the accuracy of an AI system does not mean that it will necessarily be appropriate to use, and further that the policy recognize that equality, human rights, and privacy must always be prioritized.

**Recommendation 11:**

**We recommend that** the policy classify as extreme risk AI technologies that repurpose historic, police data sets for algorithmic processing in order to draw inferences that may result in the increased deployment of police resources based on those inferences.[25]

---

[23] For example, *R v Gladue*, [1999] 1 SCR 688; *R v Ipeelee*, [2012] 1 SCR 433 at para. 60; *R v Barton*, 2019 SCC 33; *R v RDS*, [1997] 3 SCR 484; *R v Golden*, [2001] 3 SCR 679 para 83, *etc.*

[24] See for example, Danielle Ensign, Sorelle A Friedler, Scott Neville, Carlos Scheidegger, Suresh Venkatasubramanian, "Runaway Feedback Loops in Predictive Policing" (2018) 81 Proceedings of Machine Learning Research 1.

[25] Robertson, Khoo, & Song, *To Surveil and Predict*, *supra* at p. 159-160.

## 5. The TPS must not engage in unnecessary or disproportionate mass collection and analysis of data

Building on the above point, the drive towards AI accuracy can lead to increased unwarranted data collection and surveillance. TPS must resist over-collecting data, despite its availability from commercial data brokers, social media companies, and other sources. We commend TPSB for placing applications that result in mass surveillance in the extreme risk category of technologies. However, we believe that further clarity surrounding the inappropriateness of mass surveillance will strengthen the policy and better align it with fundamental human rights principles.

We begin by noting that, per that current drafting of the policy, 'discriminate' mass surveillance technologies that employ covert means would be permissible, as would indiscriminate overt mass surveillance activities. In either of these situations, using AI technologies to collect data or analyze collected data may fail to meet the tests of reasonableness, proportionality, or necessity. As such, we recommend that TPSB expand its definition of mass surveillance activity to capture the prospective harms linked with discriminate, as well as overt, mass surveillance activities. The mass collection of data itself should be identified as an extreme risk, distinct from the risk of mass surveillance and monitoring.[26] We particularly urge explicit language limiting the mass collection of data, including data from the internet and physical public and private spaces.

AI technologies can enable the analysis of data in ways that are largely inconceivable for humans to independently undertake. While mass surveillance is popularly conceived of as being associated with the collection of information, we emphasize that it can also take place when an organization undertakes a mass analysis of previously collected information. As such, we recommend that the TPSB include clearer language within the 'extreme risk' category to explicitly limit the mass collection of data, as well as the mass analysis of data previously collected, or collected without the use of an AI-system.

**Recommendations:**

**Recommendation 12:**

**We recommend that** s. 1I(i)(2) be changed to read "Where the use of the application results in mass surveillance defined as the discriminate or indiscriminate monitoring of a population or a significant component of a population".

**Recommendation 13:**

**We recommend that** the policy identify mass collection of data itself as an extreme risk, distinct from the risk of mass surveillance and monitoring, and that this risk identification explicitly include any mass collection of data, including data that may be characterized as 'publicly accessible' on the Internet or in physical public or private spaces.

[26] See for example Ian Kerr's explanation of how collection alone engages and violates privacy: "Schrödinger's Robot: Privacy in Uncertain States" (2019) 20 Theoretical Inquiries in Law 123.

**Recommendation 14:**

**We recommend that** mass data collection be defined in the policy and that there be an assessment requirement for when the TPS is collecting massive amounts of data, including but not limited to scraping content from the internet or purchasing data from data brokers.

**Recommendation 15**:

**We recommend that** the TPSB include clearer language within the 'extreme risk' category to explicitly limit the mass analysis of data previously collected, or collected without the use of an AI-system, in addition to the limit on the mass collection of data as noted in recommendation 13.

## 6. The policy should provide concrete guidance on the proactive identification and classification of risk

The policy should provide greater guidance on how to differentiate Extreme Risk Technologies from High and Moderate/Medium Risk Technologies, beyond the specific examples of technologies that would fall under the various categories currently listed in the policy. The terms moderate and medium risk were used interchangeably and we also recommend that the TPSB standardize its defined terms to be consistent with its terminology.

We recommend that further guidance be provided to assist TPSB in ensuring that risk analyses are informed by all potential sources of risk, and that risk is identified proactively instead of reactively in response to a human rights violation or a miscarriage of justice. For example, in paragraph 1(c)(i)(4), an example of an Extreme Risk technology is an application that is "known or is likely to cause harm…despite the use of mitigation techniques…". This classification itself assumes that it is sufficient to classify risk based on what is known or known to be likely, despite the history of AI systems producing unpredictable yet harmful results. Testing and vetting requirements are also relevant to the risk of a new AI-system, particularly given the possibility of unpredictable unintended harm.

For instance, the policy could identify technologies that have not been independently reviewed and scientifically validated as inherently risky as a starting point. The very absence of such independent validation leaves the possibility open that those technologies carry unknown but significant human rights risks. As noted by the Citizen Lab and IHRP in *To Surveil and Predict*, there must be robust requirements for "independent review and scientific validation (published to enable public accountability and review in court proceedings) of the underlying algorithms in policing technologies prior to their use."[27] Not only should independent validation be expressly required as a precondition to procurement and use, the absence of such validation must by definition convert a technology into an extreme or high risk technology where it may conceivably be used in a way that could touch upon human rights-protected interests.

Other forms of extreme/high risk technologies that are not mentioned in the draft policy include those high-risk technologies identified in the European Commission's draft regulation

[27] Robertson, Khoo, & Song, *To Surveil and Predict*, *supra* at p. 164.

setting out harmonised rules for the use of AI systems.[28] Risk factors identified by the European Commission such as the power imbalance between the community and the police service, and the inability of affected communities to opt-out of being affected by the system, can provide further guidance for how risk can and should be identified and classified in the TPSB policy. The draft regulation does not require *proof* of risk in order to classify a technology as risky. Instead, the regulation focuses on the *potential* for harm.

**Recommendations:**

**Recommendation 16:**

**We recommend that** the TPSB standardize its defined terms (moderate vs. medium) to be consistent with its terminology.

**Recommendation 17:**

**We recommend that** the extreme, high, and medium/moderate risk categories be more clearly defined by including factors that require proactive identification of potential risk, rather than solely relying on examples of the types of technologies that might fall into the three categories.

**Recommendation 18:**

**We recommend that** the classification of risk be based on potential for harm rather than known or proven harm caused by a technology.

**Recommendation 19:**

**We recommend that** the power imbalances between the police and the communities, as well as the inability of individuals to opt out of being assessed by the AI, both be included as factors in the proactive identification of risk of human rights impacts.

---

[28] European Commission, Proposal for a Regulation of the European Parliament and of the Council, Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, Brussels, 21.4.2021, COM(2021) 206 final ("European Commission Draft Regulation on AI"). See Annex III: High-risk AI Systems Referred to in Article 6(2).
(a) AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences; (b) AI systems intended to be used by law enforcement authorities as polygraphs and similar tools or to detect the emotional state of a natural person; (c) AI systems intended to be used by law enforcement authorities to detect deep fakes as referred to in article 52(3); (d) AI systems intended to be used by law enforcement authorities for evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences; (e) AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups; (f) AI systems intended to be used by law enforcement authorities for profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences; (g) AI systems intended to be used for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data.

## 7. This policy must ensure expertise in independent vetting, risk analysis, privacy, and human rights impact analysis

In the process of defining the conditions under which any AI-based tools can be adopted by TPS, including prohibiting the adoption of certain tools altogether, we encourage more stringent vetting of the tools themselves. We recommend that the TPSB develop requirements for the vetting, testing, and validation of new AI technologies as an integral component of this policy. We lay out this general recommendation in more specificity in the following subsections.

### a. Engaging independent expertise during the risk assessment stage of policy oversight

The language of the policy should ensure that the TPS engages independent expertise in the vetting, risk analysis, human rights analysis, and privacy impact analysis of any new AI-system. Relevant expertise includes expertise in data processing, computer systems, AI, equality, human rights, and community impacts and experiences. Integrating these interdisciplinary and intersectional perspectives will enable more fulsome assessments of the potential implications for communities who may be particularly impacted by the use of AI-based tools and algorithmic policing methods. A lack of training, resources, and capacity within police services in the complex, interdisciplinary realm of AI and human rights is a major source of risk when it comes to the introduction and use of AI technologies by those services. These technologies should not be deemed properly assessed without having first received, and implemented, recommendations from experts with the relevant and up to date expertise to undertake such assessments. Members of the impacted communities, particularly those who have been historically marginalized, will be essential in providing experiential expertise for these assessments.[29]

We commend the existing draft's inclusion of a requirement that the Chief of Police consult with experts and stakeholders in the formulation of the procedures and processes for the review and assessment of new AI technologies. However, we **recommend** that the requirement to consult with experts should also be embedded in the very risk analysis that is contemplated for the particular new AI technologies under assessment.

Similarly, we also **recommend** that the TPSB provide more direction in this policy with respect to the specific content of the risk assessment process for each AI technology. As noted in *To Surveil and Predict*, a properly conducted algorithmic impact assessment includes "meaningful public consultation that allows impacted communities, external researchers, human rights experts, and civil society to understand how technologies are being used, to identify potential issues, and to provide feedback or recommendations to relevant authorities, and to challenge the proposed or continued use of a technology where it risks infringing upon constitutional or human rights."[30] Moreover, an assessment process should operate within an established framework, including the range of factors set out in *To Surveil and Predict*, such as articulating any net benefits the technology is expected to provide to communities; articulating potential harmful impacts "including human rights impacts, sociological impacts, and material on-the-ground impacts … with particular focus on historically over-policed communities"; and outlining mitigation strategies for each of the identified potential harms—or stating if no mitigation strategies are identified or available.[31]

---

[29] Ngozi Okidegbe, *Discredited Data*, 107 Cornell L. Rev __ (forthcoming 2022).
[30] Robertson, Khoo, & Song, *To Surveil and Predict*, *supra* at 141.
[31] *Ibid.*

### b. Maintenance, auditing, and oversight of AI systems

The present draft of the TPSB policy would require the Chief of Police to review High and Moderate/Medium risk technologies every five years to determine whether there is a continued need for the technology, and to review "the quality of the AI technology, its outputs, and associated Key Performance Indicators."[32] While it is not a defined term, we infer that the "Key Performance" indicators are those referred to in paragraph 11(b) and paragraph 5(n) of the draft policy. The only guidance that is provided as to what these performance indicators may be is the statement in paragraph 5(n) that the indicators enable a determination of whether the "AI technology is achieving its intended goal and whether its deployment has had any unintended consequences." Despite the five-year incremental review, the draft policy only requires the indicators referred to in paragraph 5(n) to be tracked for a minimum of 12 months after full deployment. Paragraph 10 also states that the Chief of Police is only required to monitor high and medium risk AI technologies for a total of 12 months after full deployment.

We **recommend** that the TPSB recognize that all high and medium risk AI technologies will need to be monitored *ongoingly and indefinitely*. If AI technologies are to be used, the TPS must do so with the concurrent acceptance of full responsibility to properly maintain AI systems that risk human rights violations. The reality may well be that the resources that are required to do so are significant or costly. If that cost is a deterrent, then it should deter the use of the technology, as opposed to diluting the oversight mechanisms meant to make the use of a risky technology safer.

Furthermore, if AI technologies are adopted by police services then experts in AI systems and community human rights impacts should be involved in assessing a) how often the particular AI system will need to be reviewed, and b) how an AI system needs to be monitored and tracked in order to prevent existing error rates and bias from increasing over time. AI technologies that integrate machine learning will require more frequent and robust assessments than the currently drafted every five-year period so as to ensure that they are maintained and functioning properly. The features of a maintenance, auditing, and oversight program within a police service was the subject of a number recommendations by Citizen Lab and IHRP in Part 6 of *To Surveil and Predict*.

The draft policy incorporates a need to track unintended consequences of a technology. However, it is not clear how those unintended consequences would be identified without independent consultation as part of the ongoing monitoring and review process.

While the draft presently includes the possibility of auditing (in paragraphs 9 and 14), we **recommend** that the policy explicitly recognize that auditing is an essential feature of maintaining and monitoring an AI system.[33] Audits are necessary to ensure that incremental reviews have sufficient baseline data in order to ascertain the quality of the algorithm and its outputs over time. Internal auditing of system access logs is also needed to detect that unusual behaviour or breaches of

[32] Draft Policy s. 18(a) on p 10.

[33] By way of example, the Information and Privacy Commissioner of Ontario stated that regular reviews and audits are necessary to evaluate and improve automated license plate reader systems in Ontario: Information and Privacy Commissioner of Ontario, Guidance on the Use of Automated Licence Plate Recognition Systems by Police Services, July 2017, p. 11, online: <https://www.ipc.on.ca/wp-content/uploads/2016/09/alpr_systems.pdf> .

the policies and procedures that govern the use of the technology are identified and, if necessary, the AI system disabled or individuals responsible for a breach disciplined.

**Recommendations:**

**Recommendation 20:**

**We recommend that** a requirement to consult with experts be added to the risk analysis process that is contemplated for all new AI technologies. At present, the draft policy only requires (at paragraph 1) consultation in the development of the risk assessment procedures in general.

**Recommendation 21:**

**We recommend that** a non-exhaustive list of expertise be recognized in the policy, including members of historically marginalized communities, members of communities who have experienced or are at risk of biased assessments by AI, legal, racial justice, equality, and technology and human rights scholars, public interest technologists, and security researchers.

**Recommendation 22:**

**We recommend that** the TPSB provide more direction in this policy with respect to the specific content of the risk assessment process for each AI technology, in line with the recommendations in *To Surveil and Predict* regarding the proper content of algorithmic impact assessments.[34]

**Recommendation 23:**

**We recommend that** the TPSB recognize that all High and Moderate/Medium risk AI technologies will need to be monitored *ongoingly and indefinitely*. As such, we recommend that the one-year limit be removed from paragraphs 5(n) and 10 of the draft policy.

**Recommendation 24:**

**We recommend that** the TPSB policy require that the TPS engage external expertise when developing the monitoring and oversight mechanisms associated with specific AI and predictive policing technologies.[35]

**Recommendation 25:**

**We recommend that**, at a minimum, reviews of AI systems be conducted at least annually in addition to taking into account all expert advice on what monitoring processes will be required for a particular technology. We note that a five-year gap between reviews is an extraordinarily long time in the realm of AI research. As such, we recommend that the five-year period in paragraph 18 should be replaced with a requirement that a review be conducted "at least once every year".

**Recommendation 26:**

[34] Robertson, Khoo, & Song, *To Surveil and Predict*, *supra* at 141.
[35] Robertson, Khoo, & Song, *To Surveil and Predict*, *supra* at Recommendation 13 on p. 163.

**We recommend that** all uses of AI technology must incorporate statistical tracking and a formal documentation process for all known errors and incidents.[36] Formalizing documentation requirements is an essential aspect of effective accountability and oversight systems that focus not just on transparency but accountability as well.

**Recommendation 27:**

**We recommend that** the TPSB policy require the imposition of ongoing tracking and monitoring protocols that specifically incorporate monitoring practices that are attentive to patterns that reflect bias, with the content of that tracking to be developed in consultation with experts.[37]

**Recommendation 28:**

**We recommend that** the policy should require regular and independent auditing, with the content and frequency of those audits to be developed in consultation with experts.[38]

**Recommendation 29:**

**We recommend that** the TPSB publicly release an annual report of all unintended consequences associated with AI-systems so as to provide transparency and accountability about the operation of such systems.

## 8. The TPSB should be aware of assessment challenges that can arise when an AI system is developed by a private enterprise

This policy does not distinguish between public and private sector development of the AI systems that could be used by the TPS. Private companies may be reluctant to share information about how their system functions due to a risk of exposing their underlying code, training data, or trade secrets.[39] The current draft policy does not take this into consideration. It should include this as an assessment factor and if this information is not accessible, which is necessary to assess and explain the AI systems used by the Toronto Police, such a lack of information should elevate the risk of the technology to one which cannot be used in the context of law enforcement and investigation activities.

Questioning the results of AI-driven police decision-making must remain accessible to individuals or groups who are seeking explanations for how decisions were made about them. Law enforcement agencies have a responsibility to make it easy for impacted groups and individuals to understand how decisions were made about them, examine the decisions made by AI systems, and/or identify inequitable outcomes or related harms. Transparency, accessibility and intelligibility

[36] Robertson, Khoo, & Song, *To Surveil and Predict*, *supra* at Recommendation 14 at p. 165.
[37] Robertson, Khoo, & Song, *To Surveil and Predict*, *supra* at Recommendation 10 on p. 160.
[38] Robertson, Khoo, & Song, *To Surveil and Predict*, *supra* at Recommendation 17 at p. 167-168.
[39] See e.g. Rebecca Wexler, "Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System" (2018) 70 Stanford Law Review 1343. See also PIPEDA Finding #2021-001, *supra*.

in AI decision making are important for the development of public trust, to ensure individual dignity, and to protect equality.

The TPSB policy must ensure that the TPS does not procure or use AI systems that are not compatible with due process and accountability obligations.[40]

**Recommendations**

**Recommendation 30:**

**We recommend that** whenever TPS proposes to enter into an agreement to purchase or procure new AI systems, TPSB must require that public interest legal standards and public sector control will apply to those commercial purchases, particularly when criminal jeopardy is at stake. Companies must agree in contract to waive trade secret or other protections in pertinent circumstances, which should be well defined with a view to protecting due process and other human rights. Alternatively, TPS may develop systems in-house, and in doing so "might follow the model of the Saskatchewan Police Predictive Analytics Lab, which is developing its predictive analytics technology in-house and in partnership with academic experts, under a university research ethics protocol."[41]

**Recommendation 31:**

**We recommend that** when the TPSB is assessing the potential use of an AI system developed by a private company that could impact individual rights, if the company cannot provide its source code, training data, or other pertinent information about the system's development or ongoing operations that are needed to comprehensively explain the workings and operation of the system, the system should thus should be classified as an extreme risk (i.e. one that is prohibited).

**Recommendation 32:**

**We recommend that** if high-risk AI technologies are to be used at all, the TPS should develop their own AI system whenever possible in order to better ensure that source code and related details of that AI will be publicly available and in machine-readable and human readable forms. This information should be available to the public and to researchers.[42] Such a system must still be subject to the entire review process and requirements of the policy.

### 9. The TPSB must apply the draft policy to all existing AI technologies that are used by, or presently accessible to, the Toronto Police Service

**Recommendation 33:**

**We recommend that** the TPSB to apply any policy applicable to AI technologies to all AI technologies in the possession of, or accessible to, the Toronto Police Service. This must include the TPS' use of facial recognition technology, the TPS' collaborations with Environics Analytics, the

[40] Robertson, Khoo, & Song, *To Surveil and Predict*, *supra* at p. 165.
[41] Robertson, Khoo, & Song, *To Surveil and Predict*, *supra* at p. 165.
[42] Robertson, Khoo, & Song, *To Surveil and Predict*, *supra* at p. 169.

TPS' access to IBM's Cognos Analytics and SPSS (Statistical Package for the Social Sciences) software, or other similar technologies that may be in use but unknown to the public.[43]

As noted above, we also **recommend** that the TPSB place an immediate moratorium on law enforcement use of algorithmic policing technologies that do not meet minimum prerequisite conditions of reliability, necessity, and proportionality. As concluded in *To Surveil and Predict*, "[a] moratorium should immediately begin with facial recognition technology."[44] All AI technologies, including those already accessible to the TPS should undergo assessment to determine whether the technology is independently verified as reliable; whether the use of the technology by law enforcement authorities is necessary for the tasks performed and their stated objectives; and whether the technology is proportionate to the tasks and objectives, given associated costs, risks, and harms.

As the TPSB moves forward on developing this policy we implore the Board to centre substantive equality, human rights, and privacy protections in the content and implementation of this policy.

We are grateful for the opportunity to submit these comments and welcome any chance to discuss them further.

Sincerely,

Kristen Thomasen, Assistant Professor, Peter A. Allard School of Law, University of British Columbia

Suzie Dunn, member of LEAF's Technology-Facilitated Violence Advisory Committee; Assistant Professor, Schulich School of Law, Dalhousie University

Kate Robertson, Research Fellow, Citizen Lab; criminal and regulatory litigator, Markson Law

Pam Hrick, Executive Director & General Counsel, Women's Legal Education and Action Fund

Cynthia Khoo, Research Fellow, Citizen Lab

Rosel Kim, Staff Lawyer, Women's Legal Education and Action Fund

Ngozi Okidegbe, Assistant Professor of Law at Cardozo School of Law

Christopher Parsons, Senior Research Associate, Citizen Lab

[43] Robertson, Khoo, & Song, *To Surveil and Predict*, *supra* at p. 44-45.
[44] Robertson, Khoo, & Song, *To Surveil and Predict*, *supra* at p. 154.

## Appendix: Recommendations

**Recommendation 1:**

**We recommend that** any policies used by TPSB to govern the TPS' procurement or use of AI-based technologies include a requirement that all AI-systems must meet the minimum prerequisites of reliability, necessity, and proportionality.

**Recommendation 2:**

**We recommend that** whenever a proposed or currently used AI-system cannot meet the prerequisites of reliability, necessity, and proportionality that the technology or system should either be banned or severely limited in its uses.

**Recommendation 3:**

**We recommend that** there be clear language in the policy that allows for the outright rejection of certain AI systems and a requirement to reverse course on a technology that is already in use if it is later found to violate the prerequisites of reliability, necessity, and proportionality.

**Recommendation 4:**

**We recommend that** under s. 5(g) of the policy, reporting to the TPSB include the identification of potential individual and systemic human rights violations and harms.

**Recommendation 5:**

**We recommend that** under s. 5(h) of the policy, reporting to the TPSB include the identification of any potential human rights violations that could be caused by an AI system on an individual level as well as the identification of any potential systemic harms that could be caused or replicated by the use of an AI system (e.g. crime prediction systems).

**Recommendation 6:**

**We recommend that** when conducting the risk analysis for the AI categorization that the policy explicitly state that it will consider the privacy, equality, and human rights on an individual and systemic level. Such language might be included under s 1(c)(i)(4)).

**Recommendation 7:**

**We recommend that** the word "socioeconomic" be added after the word "gender" in paragraph (h) on page 7.

**Recommendation 8:**

**We recommend that** TPSB explicitly acknowledge that limits on and oversight of AI system use is not itself enough to ensure TPS use of such systems will not engage constitutional and human

rights. This recommendation is accompanied by the recommendations concerning vetting requirements that we discuss below in sections 6 and 7 as one mechanism for addressing some of the concerns raised here.

**Recommendation 9:**

**We recommend that** the policy include a required assessment of, and justification for, TPS collection and use of data to be processed through or otherwise utilized by algorithmic policing systems.

**Recommendation 10:**

**We recommend that** the policy recognize that the accuracy of an AI system does not mean that it will necessarily be appropriate to use, and further that the policy recognize that equality, human rights, and privacy must always be prioritized.

**Recommendation 11:**

**We recommend that** the policy classify as extreme risk AI technologies that repurpose historic, police data sets for algorithmic processing in order to draw inferences that may result in the increased deployment of police resources based on those inferences.[45]

**Recommendation 12:**

**We recommend that** s. 1(c)(i)(2) be changed to read "Where the use of the application results in mass surveillance defined as the discriminate or indiscriminate monitoring of a population or a significant component of a population".

**Recommendation 13:**

**We recommend that** the policy identify mass collection of data itself as an extreme risk, distinct from the risk of mass surveillance and monitoring, and that this risk identification explicitly include any mass collection of data that may be characterized as 'publicly accessible' on the Internet or in physical public or private spaces.

**Recommendation 14:**

**We recommend that** mass data collection be defined in the policy and that there be an assessment requirement for when the TPS is collecting massive amounts of data, including but not limited to scraping content from the internet or purchasing data from data brokers.

**Recommendation 15**:

**We recommend that** the TPSB include clearer language within the 'extreme risk' category to explicitly limit the mass analysis of data previously collected, or collected without the use of an AI-system, in addition to the limit on the mass collection of data as noted in recommendation 13.

[45] Robertson, Khoo, & Song, *To Surveil and Predict*, *supra* at p. 159-160.

**Recommendation 16:**

**We recommend that** the TPSB standardize its defined terms (moderate vs. medium) to be consistent with its terminology.

**Recommendation 17:**

**We recommend that** the extreme, high, and medium/moderate risk categories be more clearly defined by including factors that require proactive identification of potential risk, rather than solely relying on examples of the types of technologies that might fall into the three categories.

**Recommendation 18:**

**We recommend that** the classification of risk be based on potential for harm rather than known or proven harm caused by a technology.

**Recommendation 19:**

**We recommend that** the power imbalances between the police and the communities, as well as the inability of individuals to opt out of being assessed by the AI, both be included as factors in the proactive identification of risk of human rights impacts.

**Recommendation 20:**

**We recommend that** a requirement to consult with experts be added to the risk analysis process that is contemplated for all new AI technologies. At present, the draft policy only requires (at paragraph 1) consultation in the development of the risk assessment procedures in general.

**Recommendation 21:**

**We recommend that** a non-exhaustive list of expertise be recognized in the policy, including members of historically marginalized communities, members of communities who have experienced or are at risk of biased assessments by AI, legal, racial justice, equality, and technology and human rights scholars, public interest technologists, and security researchers.

**Recommendation 22:**

**We recommend that** the TPSB provide more direction in this policy with respect to the specific content of the risk assessment process for each AI technology, in line with the recommendations in *To Surveil and Predict* regarding the proper content of algorithmic impact assessments.[46]

**Recommendation 23:**

**We recommend that** the TPSB recognize that all High and Moderate/Medium risk AI technologies will need to be monitored *ongoingly and indefinitely*. As such, we recommend that the one-year limit be removed from paragraphs 5(n) and 10 of the draft policy.

[46] Robertson, Khoo, & Song, *To Surveil and Predict*, *supra* at 141.

**Recommendation 24:**

**We recommend that** the TPSB policy require that the TPS engage external expertise when developing the monitoring and oversight mechanisms associated with specific AI and predictive policing technologies.[47]

**Recommendation 25:**

**We recommend that**, at a minimum, reviews of AI systems be conducted at least annually in addition to taking into account all expert advice on what monitoring processes will be required for a particular technology. We note that a five-year gap between reviews is an extraordinarily long time in the realm of AI research. As such, we recommend that the five-year period in paragraph 18 should be replaced with a requirement that a review be conducted "at least once every year".

**Recommendation 26:**

**We recommend that** all uses of AI technology must incorporate statistical tracking and a formal documentation process for all known errors and incidents.[48] Formalizing documentation requirements is an essential aspect of effective accountability and oversight systems that focus not just on transparency but accountability as well.

**Recommendation 27:**

**We recommend that** the TPSB policy require the imposition of ongoing tracking and monitoring protocols that specifically incorporate monitoring practices that are attentive to patterns that reflect bias, with the content of that tracking to be developed in consultation with experts.[49]

**Recommendation 28:**

**We recommend that** the policy should require regular and independent auditing, with the content and frequency of those audits to be developed in consultation with experts.[50]

**Recommendation 29:**

**We recommend that** the TPSB publicly release an annual report of all unintended consequences associated with AI-systems so as to provide transparency and accountability about the operation of such systems.

**Recommendation 30:**

**We recommend that** whenever TPS proposes to enter into an agreement to purchase or procure new AI systems, TPSB must require that public interest legal standards and public sector control will apply to those commercial purchases, particularly when criminal jeopardy is at stake. Companies

[47] Robertson, Khoo, & Song, *To Surveil and Predict*, *supra* at Recommendation 13 on p. 163.
[48] Robertson, Khoo, & Song, *To Surveil and Predict*, *supra* at Recommendation 14 at p. 165.
[49] Robertson, Khoo, & Song, *To Surveil and Predict*, *supra* at Recommendation 10 on p. 160.
[50] Robertson, Khoo, & Song, *To Surveil and Predict*, *supra* at Recommendation 17 at p. 167-168.

must agree in contract to waive trade secret or other protections in pertinent circumstances, which should be well defined with a view to protecting due process and other human rights. Alternatively, TPS may develop systems in-house, and in doing so "might follow the model of the Saskatchewan Police Predictive Analytics Lab, which is developing its predictive analytics technology in-house and in partnership with academic experts, under a university research ethics protocol."[51]

**Recommendation 31:**

**We recommend that** when the TPSB is assessing the potential use of an AI system developed by a private company that could impact individual rights, if the company cannot provide its source code, training data, or other pertinent information about the system's development or ongoing operations that are needed to comprehensively explain the workings and operation of the system, the system should thus should be classified as an extreme risk (i.e. one that is prohibited).

**Recommendation 32:**

**We recommend that** if high-risk AI technologies are to be used at all, the TPS should develop their own AI system whenever possible in order to better ensure that source code and related details of that AI will be publicly available and in machine-readable and human readable forms. This information should be available to the public and to researchers.[52] Such a system must still be subject to the entire review process and requirements of the policy.

**Recommendation 33:**

**We recommend that** the TPSB to apply any policy applicable to AI technologies to all AI technologies in the possession of, or accessible to, the Toronto Police Service. This must include the TPS' use of facial recognition technology, the TPS' collaborations with Environics Analytics, the TPS' access to IBM's Cognos Analytics and SPSS (Statistical Package for the Social Sciences) software, or other similar technologies that may be unknown to the public.[53]

[51] Robertson, Khoo, & Song, *To Surveil and Predict*, *supra* at p. 165.
[52] Robertson, Khoo, & Song, *To Surveil and Predict*, *supra* at p. 169.
[53] Robertson, Khoo, & Song, *To Surveil and Predict*, *supra* at p. 44-45.