Feedback on Artificial Intelligence Procedures

The Toronto Police Services (TPS) is setting national precedent. We welcome the process to engage in public consultation around artificial intelligence procedures and recognize that the Toronto Police Services are doing what, to our knowledge, no other police force in Canada have yet completed.

Our submission:

1. Recommends a more comprehensive public consultation mechanism throughout the review process;
2. Raises concerns about the adequacy of the Artificial Intelligence Technology Committee to the goals of transparency and accountability;
3. Recommends the TPS adopt best practices for algorithmic or artificial intelligence impact assessments;
4. Encourages more attention to bias and harm;
5. Recommends clarification regarding the exceptions for disclosure; and,
6. Recommends advancing the auditing frameworks necessary for a robust procedure.

These recommendations are preliminary at best. As we discuss, the limited nature of the consultation and specific details directly impede our ability for meaningful feedback. As such:

- We strongly call upon the TPS to extend this public consultation process, and at minimum consider an expert discussion session to engage with feedback and consider improvements to this Procedure.

Consultation

Consultations are important for good governance, public literacy, and public engagement. Canada has the second lowest (32%) support for the statement “Products and services using artificial intelligence have more benefits than drawbacks” according to a 2022 Ipsos poll for the World Economic Forum.[1] We do not believe that the current online-only, one-month consultation window in December will alleviate these concerns nor legitimate the use of *machine learning* technologies in a police force that has just recently apologized for years of systemic racism. These consultations, while a good first step, fail to meet the challenges ahead.

The present mechanism of consultations as framed in the draft is insufficient to meet the risks and responsibilities associated with the effective use of AI. Effective consultation needs to elaborate

[1] See: https://www.ipsos.com/sites/default/files/ct/news/documents/2022-01/Global-opinions-and-expectations-about-AI-2022.pdf

how the public is engaged, ensure mechanisms to alleviate the biases incurred in the submission format (e.g. who has time and capacity to submit written comments and whose perspectives will be missed by that format), and create community-based formats for public engagement.

The lack of detail in the policy further undermines our capacity to meaningfully engage with the policy. Public information that clarifies the following is needed to fully assess the procedure document:

1. What sources of data will be included for internal assessment. We do not believe that vendor data will allow the TPS or the Artificial Intelligence Technology Committee (AITC) to answer key questions in the Risk Escalator, yet the information in that document will be central to decision making at an early stage of the process.
2. The specific methodologies the TPS intends to use to assess biases and risks in its different data sources that might train AI systems, or the process by which methodologies will be chosen and approved based on specificities of different technologies under consideration.
3. Any details about the Artificial Intelligence Assessment Systems.
4. Frameworks for public consultations and expectations.

Without further details the guidance that respondents to this consultation submit, including this response, is inherently incomplete.

Adequacy of the Artificial Intelligence Technology Committee

We applaud the establishment of a committee dedicated to assessing the risks and potential usages of AI technologies. AI technologies are unlike any other technologies procured by police services and require a markedly different approach to procurement and governance (e.g. see NYU 2021 AI and Procurement Primer[2], or GOV.UK on AI procurement[3]), and an expert committee is now well-established best practice.

However, in its current form the Artificial Intelligence Technology Committee is not fit for purpose. In fact, as it is currently designed, the AITC would significantly degrade the Toronto Police Service's compliance on the AI ethics principles of transparency, accountability, and justifiability — and would fall short of the TPSB's AI policy released in February 2022.

As described by the draft document, the AITC would establish its own mandate and review policy, while also being staffed entirely by TPS personnel and alone possessing the power to decide whether (not when) to include external experts, affected communities, or public engagement in its process. This procedure does not include any clear mechanisms for embedding public

[2] Sloane, M., Chowdhury, R., Havens, J. C., Lazovich, T., & Rincon Alba, L. (2021). AI and Procurement-A Primer.

[3] See: https://www.gov.uk/government/publications/guidelines-for-ai-procurement/guidelines-for-ai-procurement

contributions in the process, and so gravely undermines compliance with established AI ethics principles of inclusivity and engagement, as well as falling short of the TPSB policy on “Meaningful Engagement: The adoption of specific AI technologies must be preceded by meaningful public engagement commensurate with the risks posed by the technology contemplated.” Including independent, external experts in the AITC and embedding an obligatory public consultation with sufficient engagement capacity at the onset of the AITC’s review process would go a long way to bringing this procedure into compliance with AI ethics and establishing trust with the public.

As a result of the AITC’s current form, several crucial points of technology review seem likely to happen removed from the public view, further violating principles of transparency, accountability, and justifiability.

The AITC is responsible for evaluating the Business Initiative Review (BIR) and TPS 209, determining risk and mitigation, assessing Privacy Impact Assessments (PIAs) and Algorithmic Impact Assessments (AIAs), conducting the post-test reviews, and ensuring post-deployment re-evaluation. These are the single most important points in AI technology assessment. As currently designed, not only is it not clear to what degree this will be undertaken publicly as required by Board policy (“To the greatest degree possible, the Board must conduct such reviews in public”), but there is no description of the ways in which the frameworks, metrics, and procedures by which the assessment is undertaken will be made public.

Publicity is necessary to comply with the Board policy that the TPS “will make the procedures required under section 1, including a detailed risk assessment tool, available to the public on the Service’s website.” It is not sufficient that the outcomes of the AITC’s review are made available to the Board at the end of the review process. At the very least, the entire process and all tools used within it need to be publicly accessible. However, to properly comply with AI ethics, the design and usage of those tools should be done in meaningful consultation with external AI experts and affected communities.

By enshrining this procedural structure in policy, the AITC is actually a step backwards for the TPS’s claim to be “committed to:”

- “continuously ensuring bias is avoided in all new AI technology,”
- ensuring that “the ethical, legal and community impacts of all new AI technology will be thoroughly reviewed to ensure legal compliance and transparency to the public”
- and to “ensuring the protection of individual liberty and operating in accordance with the law.”

We applaud the TPS and the TPSB’s actions to develop AI policy, but now is the time to open up the space for public debate and so build deep trust in our institutions and strategies going forward, not to foreclose this process after it has barely begun.

Best practices Artificial Intelligence Assessment

There are minimal details on what the BIR, TPS 209, testing, stakeholder consultation, AIA, and PIA will look like and what type of information will be gathered from each of these stages for AITC's decision-making.

Putting aside the lack of transparency and clarity on the nature of these assessments, the Artificial Intelligent Assessment (AIA) and Privacy Impact Assessment are conducted too late in the proposed TPS procedure. These assessment processes, if done correctly, reveal critical information that would be necessary for all the six prior stages prior including to the BIR & AI screening, AITC review, the decision of whether the AI application is sensitive, testing and stakeholder consultation, and AITC evaluation.

There are no details given about the PIA process. However, few details are shared about the AIA process, and below we discuss how each of these pieces of information is necessary earlier in the TPS process. According to the TPS procedure, the AIA requires the inclusion of:

- *"a functional description of the AI and the processes and decisions it is acting upon* '': This piece of information is necessary for deciding whether a particular AI technology is fit for a specific business need and it needs to be known before BIR and must be included in TPS 209.
- "*Description of any biases and limitations, and methods to mitigate" and "results of any testing or reviews"*: This kind of information will be absolutely necessary for determining whether an AI application is sensitive or not sensitive considering that "Sensitive refers to AI technology that has the potential to impact *rights*, *privacy*, *marginalization* or *discrimination*". There is a rapidly growing body of research on the assessment of fairness and bias-related issues of AI systems[4,5] and these initial assessments could be used earlier on in the TPS procurement process to determine potential biases before making a decision on sensitivity, further testing, and stakeholder consultation. Furthermore, a decision on the sensitivity of an application requires the results from a PIA.
- *"a description of the data used by the application, or in lieu of a description may provide a link to the website when the data is publically available":* The information about the data used is critical for understanding AI technology and mapping the potential risks that it could cause. The criticality of understanding data sources has been well documented in the

[4] Ninareh Mehrabi, Fred Morstatter, Nripsuta Saxena, Kristina Lerman, and Aram Galstyan. 2021. A Survey on Bias and Fairness in Machine Learning. ACM Comput. Surv. 54, 6 (2021). DOI:https://doi.org/10.1145/3457607

[5] Kiana Alikhademi, Emma Drobina, Diandra Prioleau, Brianna Richardson, Duncan Purves, and Juan E. Gilbert. 2022. A review of predictive policing from the perspective of fairness. Artif. Intell. Law 30, 1 (2022), 1–17. DOI:https://doi.org/10.1007/s10506-021-09286-4

literature[6] and there is a growing body of research on establishing appropriate data provenance for AI technology[7]. The information on what data is used to train and test AI technology and how this data can shift while a given AI technology is in use is necessary for the initial AITC review and decision-making on whether an application is sensitive.

- *"An evaluation of the relevant data security, with mitigation and assessment recommendations":* An evaluation of data security protocols for a given AI technology needs to be considered as part of the initial AITC review. If a particular AI technology provider does not have proper data security protocols in place, their product can pose a significant result for any given application.

As illustrated, the information elicited in the AIA is needed much earlier on in the TPS procedure. Furthermore, the elements of the AIA process as described in the TPS procedure are insufficient as it does not include any assessment of data collection and preparation processes for creating a given AI technology, the efficacy of the algorithms used in an AI technology, and how potential stakeholders would be impacted and harmed by an AI technology. All of this information is necessary for understanding the potential risk of AI technology on impacted stakeholders and devising appropriate ways to evaluate and mitigate such risks.

The TPS procedure can benefit tremendously from the rapidly growing body of scholarly work in responsible AI development.

We propose that the AIA and PIA are viewed as long-term and iterative processes that begin with BIR and are completed incrementally throughout the TPS procedure until the final AITC and TPSB approval. Furthermore, these processes need to be revisited after a system has been acquired at timely internals.

Considering the developing best practices in the industry and academic circles we recommend the following elements as part of the AIA process:

- The AIA process should start at the "BIR and AI screening" stage and it should include the following components (examples provided in referenced literature):
    - Functional description of the AI system and how it will be used

[6] Nithya Sambasivan, Shivani Kapania, and Hannah Highfll. 2021. Everyone wants to do the model work, not the data work: Data cascades in high-stakes ai. Conf. Hum. Factors Comput. Syst. - Proc. (2021). DOI:https://doi.org/10.1145/3411764.3445518

[7] Karl Werder, Balasubramaniam Ramesh, and Rongen Sophia Zhang. 2022. Establishing Data Provenance for Responsible Artificial Intelligence Systems. ACM Trans. Manag. Inf. Syst. 13, 2 (2022). DOI:https://doi.org/10.1145/3503488

- Data used for creating the AI system using toolkits such as data cards[8] and datasheets[9]
- High-level overview of models and algorithms used for creating the AI system using toolkits such as model cards[10,11]
- A breakdown of potential stakeholders, impacts and harms[12]. Algorithmic Impact Assessment frameworks[13] could be used to help shape an analysis of potential impacts and harms. Moss et al. highlight 10 key components that need to be considered when conducting an Algorithmic Impact Assessment based on studying well-established impact assessment frameworks. [14]

This information needs to be elicited from the AI system provider and this information should provide adequate detail to comprehensively answer whether an AI system application is sensitive or not. AITC should consider that the above information will also clarify the type of testing and stakeholder consultation necessary for sensitive applications. We strongly recommend that the AITC updates the AIA after further testing and stakeholder consultation. There are many emerging testing and stakeholder engagement practices in the industry[15] and these need to be considered when designing testing and stakeholder engagement processes. For example, Solon et al. describe an emerging best-practice process of conducting disaggregate analysis for AI systems to investigate how well a system operates for different user groups using a range of performance metrics[16]. Including these types of analyses would be valuable in the testing phase. Furthermore,

---

[8] 2022. Data Card Playbook. Google Research. Retrieved from https://sites.research.google/datacardsplaybook/

[9] Timnit Gebru, Jamie Morgenstern, Briana Vecchione, Jennifer Wortman, Vaughan Hanna, Hal Daumé, and I I I Kate. 2018. Datasheets for Datasets. (2018).

[10] 2020. Model Cards. Google Cloud. Retrieved from https://modelcards.withgoogle.com/about

[11] Margaret Mitchell, Simone Wu, Andrew Zaldivar, Parker Barnes, Lucy Vasserman, Ben Hutchinson, Elena Spitzer, Inioluwa Deborah Raji, and Timnit Gebru. 2019. Model cards for model reporting. FAT* 2019 - Proc. 2019 Conf. Fairness, Accountability, Transpar. Figure 2 (2019), 220–229. DOI:https://doi.org/10.1145/3287560.3287596

[12] Renee Shelby, Shalaleh Rismani, Kathryn Henee, Ajung Moon, Negar Rostamzadeh, Paul Nicholas, N', Mah Yilla, Jess Gallegos, Andrew Smart, Emilio Garcia, and Gurleen Virk. 2022. Sociotechnical Harms: Scoping a Taxonomy for Harm Reduction. Association for Computing Machinery, 1–29. Retrieved from https://arxiv.org/abs/2210.05791v1

[13] Jacob Metcalf, Emanuel Moss, Elizabeth Anne Watkins, Ranjit Singh, and Madeleine Clare Elish. 2021. Algorithmic impact assessments and accountability: The co-construction of impacts. FAccT 2021 - Proc. 2021 ACM Conf. Fairness, Accountability, Transpar. (2021), 735–746. DOI:https://doi.org/10.1145/3442188.3445935

[14] Metcalf, Jacob, Moss, Emanuel, Watkins, Elizabeth Anne, Singh, Ranjit, Elish, Madeleine Clare. 2022. Assembling Accountability: Algorithmic Impact Assessment for the Public Interest. Retrieved from https://ssrn.com/abstract=3877437

[15] Bogdana Rakova, Jingying Yang, Henriette Cramer, and Rumman Chowdhury. 2021. Where Responsible AI meets Reality: Practitioner Perspectives on Enablers for Shifting Organizational Practices. Proc. ACM Human-Computer Interact. 5, CSCW1 (2021), 1–23. DOI:https://doi.org/10.1145/3449081

[16] Solon Barocas, Anhong Guo, Ece Kamar, Jacquelyn Krones, Meredith Ringel Morris, Jennifer Wortman Vaughan, W. Duncan Wadsworth, and Hanna Wallach. 2021. Designing Disaggregated Evaluations of AI

participatory methods[17] as discussed by Beede et al. could be used to guide stakeholder engagement processes and such methods are becoming more widely used given adequate resources.

The results from testing and stakeholder engagement phases need to be used to update the Artificial Intelligence Assessment before a final decision is made about the procurement of the AI system.

Exceptions for disclosure

At present, the Procedure promises to "maintain a publicly available listing of approved technologies," a so-called AI registry. This is considered best practice in AI governance across the globe. However, the Procedure immediately undermines this policy by stating that "Where the product is covert in nature the product and vendor may be omitted. Where public disclosure of the product or details of the product may impact economic, intellectual property, or other interests, such information may be omitted pursuant to sections 10 and 11 of the Municipal Freedom of Information and Protection of Privacy Act." These exemptions need to be further refined to ensure they do not become overly broad and withhold necessary information to the public. The default should be explicitly for publication and the policy should specify that exceptions are expected to be rare. In cases where vendors require secrecy as a contractual obligation, this should be a significant point against them in the specific technology evaluation process.

Limited Auditing Framework

We are encouraged to see procurement being identified as a major point of leverage in addressing the potential impact of AI systems. This initial focus on procurement demonstrates valuable continuity between citizen input, TPSB Use of Artificial Intelligence Technology Policy and TPS implementation procedures. However, implementing a procurement procedure without an accompanying audit framework limits the effectiveness of the intended policy and procedural outcomes. The TPSB Use of Artificial Intelligence Technology Policy specifically lists audits as a required mechanism, e.g. "Ensure that any use of the AI technology will be audited to ensure adequate and lawful use, in accordance with the purposes approved by the Board, and to monitor errors; and,...". However, the draft TPS procurement policy does not provide an audit framework

---

Systems: Choices, Considerations, and Tradeoffs. Association for Computing Machinery. DOI: https://doi.org/10.1145/3461702.3462610

[17] Emma Beede, Elizabeth Baylor, Fred Hersch, Anna Iurchenko, Lauren Wilcox, Paisan Ruamviboonsuk, and Laura M. Vardoulakis. 2020. A Human-Centered Evaluation of a Deep Learning System Deployed in Clinics for the Detection of Diabetic Retinopathy. Conf. Hum. Factors Comput. Syst. - Proc. (2020), 1–12. DOI:https://doi.org/10.1145/3313831.3376718

and buries audits as an optional item under reviews: “the AITC policy outlining information to ensure a thorough review is conducted for all new AI technology
Note: this could include: terms of service; independent third party audits...”.

There are two types of audits required for effective governance of AI in law enforcement applications, technology audits and policy audits. Both technology and policy audits ensure that intended outcomes are being achieved. An effective audit framework in this case must make distinction between technology audits and policy audits. Technology audits are the first line of mitigation against risks in AI applications. Technology audits determine for example if the AI technology audited includes biases for specific groups. We request the TPS policy and procedure developers to keep abreast of critical research developments in AI technology audits and more importantly make technology audits a concrete requirement rather than an option in TPS AI technology procurement policy.[18] We also request TPS policy and procedure developers to gain an understanding of the different demographic characteristics of Canadians that make AI technology audits performed exclusively with US or European or Asian population data as invalid for a Canadian context.

The second type of audit required in this case is a policy and procedure audit. These audits are not focused on the technology itself, and ensure that procedures are being followed and policy outcomes are being achieved as intended, and are often described as compliance audits. An example of a publicly available compliance audit is the Office of the Auditor General of Ontario report on the Operation of the Environmental Bill of Rights.[19] Policy and procedure audits ‘close the loop’ and identify corrective actions to be implemented, including changes to the procedures and policies. Without policy and procedure compliance audits there is no effective feedback and no holistic governance of policies and procedures. For example, without compliance audits we would not know how often the procedure was contravened or followed. Therefore audit frameworks are not an optional review item but a required part of policies and procedures. We request TPS policy and procedure developers to include required annual compliance audits as part of the procedure to ensure that the policies and procedures are being implemented as intended. Finally, we encourage TPS policy and procedure developers to consider technology audits and procedural compliance audits as part of an integrated audit framework that requires appropriate explicit guidance and adequate resources.

[18] Costanza-Chock, S., Raji, I. D., & Buolamwini, J. (2022, June). Who Audits the Auditors? Recommendations from a field scan of the algorithmic auditing ecosystem. In 2022 ACM Conference on Fairness, Accountability, and Transparency (pp. 1571-1583); Raji, I. D., Xu, P., Honigsberg, C., & Ho, D. (2022, July). Outsider oversight: Designing a third party audit ecosystem for ai governance. In Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society (pp. 557-571).
[19] Office of the Auditor General of Ontario (2022, December). Operation of the Environmental Bill of Rights, 1993. Retrieved from:
https://www.auditor.on.ca/en/content/annualreports/arreports/en22/ENV_EBR_en22.pdf

Insufficient attention to bias and no mention of harm

The document mentions that "The Service is committed to continuously ensuring bias is avoided in all new AI technology being considered." This statement is limited to *new* AI technology being considered. Addressing bias in *existing* AI technology is equally important. There also is the issue that the TPS definition of bias (see p. 7 of draft procedure) does not capture geographic bias like postal codes that simultaneously reflect racial bias. It also does not capture algorithmic bias, which can include optimization, efficiency, performance (e.g., determining what percentage of false positives or false negatives are acceptable).

We reiterate that, unfortunately, bias in policing data cannot be avoided. If the AI requires training data then that training data relies on historical data. In the case of policing, there is well-founded skepticism for thinking that an effective and fair tool could be built within a system that is historically racist and contains other biases.[20] Research on predictive policing has shown that AI policing technology can all too easily be trained on "dirty data". [21] Dirty data can reflect "police departments' conscious and implicit biases, as well as police corruption."[22] Evidence shows that predictive policing software is discriminatory in its over-prediction of the likelihood of black people committing future crimes, and significant under-prediction of white people, especially when compared to black people[23], and can be viewed as "crime production algorithms".[24] So statements like "The Service is committed to continuously ensuring bias is avoided" offer a false promise.

Bias cannot be avoided, it can only be reduced. One way to do this is by using methods to computationally debias data. However, there are flaws in using a computer to correct the flaws of human beings. For example, Prost et al. (2019) found that debiasing techniques could worsen gender bias.[25] More recent arguments ask us to move beyond arguments around bias/debiasing to harm since debiasing alone does not guarantee fairness, equality and non-discrimination.[26] Instead

---

[20] Heilweil, R. (2020, February 18). Why algorithms can be racist and sexist. Vox. Retrived from https://www.vox.com/recode/2020/2/18/21121286/algorithms-bias-discrimination-facial-recognition-transparency

[21] Richardson, R., Schultz, J. M., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. *NYU Law Review. Online*, *94*, 15.

[22] Heilweil, R. (2020, February 18). Why algorithms can be racist and sexist. *Vox*. Retrived from https://www.vox.com/recode/2020/2/18/21121286/algorithms-bias-discrimination-facial-recognition-transparency

[23] Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). Machine bias. In *Ethics of Data and Analytics* (pp. 254-264). Auerbach Publications.

[24] Benjamin, R. (2019). *Race after technology: Abolitionist tools for the New Jim Code.* Polity, p. 83.

[25] Prost, F., Thain, N. & Bolukbasi, T. (2019). Debiasing embeddings for reduced gender bias in text classification. In *Proceedings of the First Workshop on Gender Bias in Natural Language Processing*, pages 69–75, Florence, Italy. Association for Computational Linguistics.

[26] Balayn, A., & Gürses, S. (2021). Beyond Debiasing: Regulating AI and its inequalities. Report of European Digital Rights Association, Brussels. https://edri.org/wp-content/uploads/2021/09/EDRi_Beyond-Debiasing-Report_Online.pdf

of using public funds for technological solutions, “authorities should focus on fixing biases within the police and criminal justice systems."[27]

We need to look beyond the data to the algorithm to also see its potential harm. Most facial recognition technology uses a technique that essentially creates triangles out of people’s faces. These “tessellations” do not easily capture fine changes in flatter faces or faces that have been changed due to plastic surgery[28] or hormone replacement therapy.[29] The algorithms chosen to model the face can produce harm and, in the case of Uber mentioned above, “undermined [their] stated commitment to more inclusive and equitable practices".[30]

Most AI is an exercise in “information loss”, where algorithms and models reduce input data processing to something actionable. However, algorithm choice in that information reduction can induce harm. Even “relatively simple” machine learning like stepwise probit regression can be controversial because it relies only on the most correlated variables and discounts the rest to build the model. Consequently, methods can result in a “statistical fishing expedition.”[31] For police this can mean narrowing down variables to analogues to race and poverty (e.g., the neighbourhood you live in), “pluck[ing] out any variables that vary along with the thing you are trying to measure.”[32]

This Procedure could fail to properly assess ClearviewAI

The TPSB policy released in February 2022 and this subsequent TPS Procedure document are direct responses to the Clearview AI scandal. This is not per se a mark against them, most significant policy change happens as the result of an external shock. However, the external shock that the TPSB and the TPS should be considering here isn’t Clearview AI, nor is it even AI. AI isn’t a single technology; it is a number of different systems of data analytics that involve an autonomous adaptive capacity and an automated decision making component, and that crucially also involve significant systems change to all other digital technology and data systems in their ecosystem, and, as a result, to the structure of society as a whole. It is this change that should be the shock.

---

[27] Statement made by Sherrilyn Ifill, president of the NAACP Legal Defense Fund’s statement at AI Now’s 2018 symposium, “Ethics, organizing and accountability.” Retrieved from https://ainowinstitute.org/ainow-program-2018.pdf

[28] Ali, A. S. O., Sagayan, V., Malik, A., & Aziz, A. (2016). Proposed face recognition system after plastic surgery. IET Computer Vision, 10(5), 344-350. https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-cvi.2014.0263

[29] Hussain, S. (2021, December 10). Uber blocks transgender drivers from signing up: ‘They didn’t believe me’. Retrieved from https://www.latimes.com/business/technology/story/2021-12-10/uber-transgender-drivers-blocked-accounts-rejected-ids

[30] Ibid.

[31] Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press, p. 144.

[32] Ibid.

The Procedure as it stands might fail to prevent the use of Clearview AI itself. By focusing on the way in which officers first acquired Clearview AI, and not on a more comprehensive process of technology review, there are a number of points at which the Procedure would still fail to prevent a technology as harmful and illegal as Clearview AI from being adopted:

1. The initial steps of the Procedure are, in reality, the completion of the TPS 209 and its movement up the chain to the AITC. However, at no point in these steps does anyone have sufficient information or competence to properly fill out the TPS 209, and as a result it will contain only the talking points provided by the vendor itself. The joint investigation by Canadian privacy regulators demonstrated clearly the inadequacy of the likely Clearview AI talking points during a sales conversation.[33]
2. This process would ensure that the misinformation that was provided would rise unimpeded up the decision chain until step 10, when the AITC evaluates the TPS 209. However, as the AITC does not have the power to compel more information from the private company to properly assess the algorithm or training or evaluation data used, nor does it include external experts or affected communities, there is a significant chance it would fail to appropriately assess the public scraping of biometric data as illegal under Canadian law and not be able to properly determine the biases and risks in this facial recognition algorithm.
3. As a result, the process would continue. At this point the Procedure document is unclear: In contradiction to the flow chart, step 10 does not say that a “sensitive” classification would necessarily lead to stakeholder consultation, nor does it say what that stakeholder consultation would entail. As a result of this and the previous failure to uncover the serious risks, the process would likely move on to testing where the previously insufficient risk assessment and lack of publicly established frameworks and tools could well enable a passing grade once again. In other words, even an illegal tool might well seem to work on a technical level.
4. The next step is PIA/AIA. As the Procedure document does not provide a public description of what these would entail, it is difficult to assess whether the intended methodologies would identify Clearview AI’s risks. If they are well conceived, they should, but a simple analysis of collection practices, to the extent that the analyst relied on Clearview AI’s assertions that the data they collected were “publicly available” might fail again to identify the problematic nature of that particular AI tool. Should that be the case, the AITC would still be unaware of the fundamental harms and illegality of Clearview AI’s training process.

[33] Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d’accès a l’information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta. PIPEDA Findings #2021-001. Available: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/

5. Having passed the assessment process, and at best been approved with some mitigation requirements that wouldn't in actuality mitigate the real harms, the AITC's assessment would be packaged and sent to the board. At this point, the board and the public have no insight into how the assessment was reached and as such are in no position to make an independent judgment.
6. Clearview AI is adopted.

We are well aware that developing a comprehensive, rigorous, and ethical AI assessment process is extremely difficult. There are new books, articles, and reports being published on this topic every month. We once again applaud the TPS and TPSB for taking a step in this direction, and once again implore them to extend the public consultation and enable serious engagement, workshopping, and debate of the Procedure. This issue is far too important to be reduced to a process like this one.

Signatories (in alphabetical order)

Ana Brandusescu
PhD Student
Department of Geography
McGill University

Maurice Jones
PhD Student
Centre for Interdisciplinary Studies in Society and Culture (CISSC)
Concordia University

Thomas Linder, PhD
Coordinator, Knowledge and Insight Development
OpenNorth

Fenwick McKelvey
Associate Professor, Communication Studies
Concordia University

Alex Megelas
PhD Candidate, Department of Integrated Studies in Education (DISE)
McGill University

Ushnish Sengupta
Assistant Professor

Community Economic and Social Development
Algoma University

Renée Sieber
Associate Professor
Department of Geography
McGill University

Shalaleh Rismani
PhD Candidate
Department of Electrical and Computer Engineering
McGill University