Comments regarding proposed AI policy

Table of Contents

[Summary 1](#_Toc88946221)

[What the policy should be 2](#_Toc88946222)

[Guiding Principles 2](#_Toc88946223)

[Purpose of Policy 2](#_Toc88946224)

[Definitions 3](#_Toc88946225)

[Monitoring and Reporting 7](#_Toc88946226)

[Continuous Review 8](#_Toc88946227)

[Justification for edits 9](#_Toc88946228)

[Edits 1, 2 9](#_Toc88946229)

[Edit 3 12](#_Toc88946230)

[Edit 4 13](#_Toc88946231)

[Edit 5, 7 13](#_Toc88946232)

[Edit 6 13](#_Toc88946233)

[Potential use cases and their impact on policy 13](#_Toc88946234)

[Network centric “responsive” policing 13](#_Toc88946235)

[Leveraging AI tools to anticipate and circumvent organized threats to public safety (Predictive Policing) 15](#_Toc88946236)

[References 16](#_Toc88946237)

# Summary

Given the primitive state of Toronto police technology, this policy is more than sufficient to cover police usage of AI tools and data over the next five years. Additional policy should be added to protect the presumption of innocence, and to ensure individuals have the right and ability to easily see any data or conclusions collected by AI tools on themselves only. Specific demographics should not be mentioned in the policy as that gives those groups special rights. Finally, oversight of AI tools and information should be done by a committee selected in a similar format to juror selection, to prevent politicians from abusing the data within to further their own purposes.

## What the policy should be

### Guiding Principles

Novel technologies making use of artificial intelligence (AI) applications hold the promise of

improving the effectiveness of policing services and increasing public safety in Toronto. At the

same time, technological advancements may pose new concerns for the privacy, rights

(including the rights to freedom of expression, freedoms of association and freedom of

assembly), dignity and equality of the individuals affected by them. For example, there have

been instances in which novel technologies were shown to incorporate and perpetuate pre-existing and systemic biases, resulting in both individually and systemically discriminating

decisions. Furthermore, such unintended consequences may undermine the desired benefits to

efficiency and effectiveness of policing services, as well as public trust in policing. The Toronto

Police Services Board (the Board) supports the efforts of the Toronto Police Service (the Service)

and its Members to provide effective and accountable policing through the prudent adoption of

new technologies, while, at the same time, ensuring transparency and making certain that

policing is provided in accordance with both the law and the interests of the public, and protects

and promotes fundamental rights.

Under s. 41(1)(a) of the Police Services Act (the Act), the Chief of Police is responsible for

administering the police service and overseeing its operation, in accordance with the objectives,

priorities and policies established by the Board. As such, it is important for the Board and Chief

to engage in a constant dialogue about how technology will be procured, implemented and used

in the provision of policing in Toronto.

The Board is the entity that is responsible for the provision of adequate and effective policing

under the Act and its successor legislation. No current legislation fully regulates the use of AI

technologies, and the Province has not yet developed comprehensive guidelines for the use of

such technologies in policing. As a result, the Board must consider new technologies utilizing AI

that the Service intends to use in the provision of policing in Toronto, and establish policies with

regard to the use of such technologies, as needed. In its review, the Board will consider the need

for and benefits of deploying the new technology; the potential unintended consequences to

the privacy, rights, freedoms and dignity of members of the public, and to the equitable delivery

of police services to the public; and any possible mitigating actions to eliminate any such

unintended consequences. To the greatest degree possible, the Board must conduct such

reviews in public.

### Purpose of Policy

The purpose of this Policy is to ensure that the Board, as the oversight body representing the

public interest in providing policy direction to the Chief of Police, is involved in the consideration

of the use of new or enhanced technologies using AI, or of previously approved technology that

is to be used for a novel purpose or in a novel circumstance, and to establish a protocol for

reporting to:

 Preserve the privacy, rights and dignity of individuals and communities, in accordance

with the Ontario Human Rights Code, the Canadian Charter of Rights and Freedoms, and

any other applicable legislation;

 Ensure that the adoption of new technologies is done in a transparent and trustworthy

manner, and results in the advancement of equitable and effective policing services for

all members of the public;

 Ensure that consideration is given to possible unintended consequences of the use prior

to the adoption of new technologies in the provision of policing services in Toronto;

 Ensure that appropriate consultations precede the procurement and deployment of new

technologies that may have negative impacts on members of the public or the quality of

policing services in Toronto;

 Develop mitigation strategies to eliminate any unintended negative consequences from

the use of new technologies; and

 Ensure that a pre- and post-deployment evidence-based evaluation and re-assessment

takes place.

Ensure that individual rights to freedom of expression are protected, and that AI tools do not make decisions based on political viewpoints. (edit 1)

Ensure that the information and recommendations obtained from AI tools cannot be used by politicians to further their own agenda. (edit 2)

This Policy will ensure the thoughtful consideration of the benefits and risks of obtaining and

deploying any new technology using AI, or novel uses of existing technologies, including impacts

on public trust in the Service, community safety and sense of security, individual dignity, and

equitable delivery of policing services. ~~In particular, it will help to ensure that new technologies~~

~~do not introduce or perpetuate biases, including biases against vulnerable populations such as~~

~~people with disabilities, children and older persons, Indigenous, Black and racialized~~

~~communities, low-income and LGBTQ2+ communities, into policing decisions~~. (edit 3) The policy will ensure that new technologies do NOT interfere with or hamper the constitutional rights of citizens, and that the presumption of innocence will always be protected.

### Definitions

For the purpose of this Policy, the following definitions will apply:

AI Technology: goods and services, including but not limited to software and electronic devices,

which collect information about members of the public or their actions, including personal

information as defined under the Municipal Freedom of Information and Protection of Privacy

Act, or make use of existing information about members of the public or their actions, and which

use automated analytical problem-solving models to assist or replace Service Members in

identifying, categorizing, prioritizing or otherwise making decisions pertaining to the information

or the members of the public to which it pertains. AI technology includes, but is not limited to,

machine learning technology, neural networks, natural language processing applications,

predictive technologies, and computer vision. Without limiting the foregoing, for the purpose of

this policy, “AI technology” will also include any goods or services whose procurement,

deployment or use require that a privacy impact assessment be conducted in advance of their

deployment or use.

New AI technology: any of: (1) AI technology never used before by the Service, (2) goods and

services, including but not limited to software and electronic devices, already or previously

employed by the Service which are enhanced through the application of AI in a manner that

transforms the goods or services into an AI technology; (3) AI technology already or previously

employed by the Service which is being considered for deployment for a novel purpose or in

novel circumstances that may substantially change the data collected or used, including the

content of the data, its granularity, and the purpose of data collection and use; (4) AI technology

already or previously employed by the Service which is being enhanced through the use of new

data that is substantially different from the data previously used, including the type of data, its

granularity, or the manner in which it is obtained; and (5) the linking of data from existing sources

of information to create a new dataset for use by an AI technology.

Bias: consistently flawed output that is affected by flaws in the design of the AI technology or

training data, to either misidentify certain types of subjects, or ascribe them with characteristics

that disadvantage them based on illegitimate grounds (e.g., Code protected grounds).

Data: any information collected and stored, whether locally or by a third party, which is used by

the AI technology for the purpose of training, validation, testing, or generating output.

Biometrics: data on the measurements of physical and behavioural features of individuals (e.g.,

facial features, voice, gait) that could be used to identify the individual.

Human in the Loop: a process that ensures that any decisions or classifications made by the

technology must be confirmed by a human who can compare the input data with the output

decision or classification, prior to any action taking place based on the output.

Training data: data provided to the AI technology for the purpose of enabling it to learn patterns

and independently develop decision making algorithms.

Transactional data: data which is entered into a system which uses AI and that is used to generate

output, but is not leveraged for training.

Policy of the Board

It is the policy of the Toronto Police Services Board that the Chief of Police:

Review and Assessment of New AI Technologies

1. Will develop, in consultation with experts and stakeholders, procedures and processes

for the review and assessment of new AI technologies that will, at a minimum, establish:

(a) That Service Members may not use new AI technologies prior to receiving

approval in accordance with the procedure(s) and process(es);

(b) That all Service Members must be trained to identify new AI technologies for the

purpose of obtaining an approval in accordance with section 1(a);

(c) Risk categories for new AI technologies that include, at a minimum:

i. Extreme Risk Technologies, which may not be considered for adoption,

including:

1. Any application where there is no “human-in-the-loop”. A human

must evaluate a recommendation from an AI tool before

consequential action is taken;

2. Where use of the application results in mass surveillance defined

as the indiscriminate covert monitoring of a population or a

significant component of a population;

3. Any application of AI in a life-safety situation, i.e., an application

where the action of the AI technology could slow down the

reaction time of the human operator, resulting in potential risk to

life of members of the public or Service Members;

4. Any application known or is likely to cause harm or have an impact

on an individual’s rights, despite the use of mitigation techniques,

due to bias or other flaws; or

5. Where training or transactional data is known or thought to be

illegally sourced or where it is from an unknown source;

ii. High Risk Technologies, including:

1. Where training or transactional data is known to be of poor

quality, carry bias, or where the quality of such data is unknown;

2. Where training data can be influenced or biased by malicious

actors;

3. Applications which link biometrics to personal information (e.g.

facial recognition); or

4. Where a system cannot be fully explainable in its behaviour;

iii. Moderate Risk Technologies, including:

1. Where the “human-in-the-loop” may have difficulty identifying

bias or other decision failures of the AI; or

2. Where the process involved suggests an allocation of resources;

iv. Low Risk Technologies, including any AI technology that both:

1. Does not fall under the categories of Extreme High Risk, High Risk,

or Moderate Risk, and

2. Assists Members in identifying, categorizing, prioritizing or

otherwise making decisions pertaining to members of the public;

and

v. Minimal Risk Technologies, including any AI technology that does not fall

under any of the preceding categories;

(d) The minimum risk analysis and privacy impact analysis that must be carried out

for each level of risk in accordance with above subsection (c), as determined by

an initial risk analysis, and the appropriate tools to carry out such impact

analyses; and

(e) The harm mitigation measures required for each level of risk (e.g., training,

contingency planning);

2. Will make the procedures required under section 1, including a detailed risk assessment

tool, available to the public on the Service’s website;

Board Approval and Reporting Prior to Procurement, Utilization and Deployment

3. Will not procure, utilize or deploy a new AI technology deemed to be of extreme risk;

4. When contemplating procuring, utilizing or deploying new AI technology in the field, will

conduct a risk assessment of the AI technology and report to the Board where the AI

technology is found to be of high or moderate risk, prior to the earlier of:

(a) Seeking funds for the new technology, including but not limited to applying for a

grant, or accepting municipal, provincial or federal funds, or public or private inkind or other donations;

(b) Acquiring the new technology, including acquiring such technology without the

exchange of monies or other consideration;

(c) Using or deploying existing technology:

i. for a novel purpose;

ii. in novel circumstances, that may substantially change the data collected,

including the content of the data, its granularity, and the purpose of data

collection or use;

iii. for a purpose or in a manner not previously approved by the Board; or

iv. for a purpose or in a manner not practiced before the approval of this

Policy; or,

(d) Entering into agreement to acquire, share, or otherwise use such technology;

5. When reporting to the Board in accordance with section 04, will describe, at a minimum:

(a) The operational need(s) the AI technology will address, including how use of the

new AI technology will improve on current practices;

(b) How the Service intends to use the AI technology;

(c) The risk level ascribed to the AI technology, why the AI technology was ascribed

this risk level, and the rationale for continuing with the procurement, utilization

or deployment requested despite the associated risk(s);

(d) The legislative authority for the collection of personal information

(e) How the AI technology operates, including, where applicable, what information

will be collected, how information will be stored and how it will be disposed of,

and evidence of the validity and accuracy of the AI technology under

consideration;

(f) The steps the Service will take or has taken to ensure the AI technology is used

only in accordance with applicable privacy laws, the Human Rights Code and the

Charter of Rights and Freedoms and other legislative and legal requirements,

including training, and governance structures;

(g) The results of any privacy impact and other assessment(s) that have been

conducted, and consultations with the Information and Privacy Commissioner of

Ontario, the Ministry of the Attorney General and other stakeholders,

independent human rights, legal and technology experts and affected

communities, as appropriate in light of the potential risks posed by the

contemplated technology;

(h) An analysis of possible unintended consequences of the proposed use of the AI

technology, including possible effects on procedural fairness, due process, gender

and race equality, or disproportionate impacts on Human Rights Code protected

groups, and steps the Service will take to mitigate these unintended

consequences;

(i) Where applicable, a legal analysis of potential challenges to the admissibility of

evidence generated or impacted by the AI technology in criminal proceedings;

(j) The findings of any risk analyses carried out in accordance with section 1(d)

above, and any additional analysis as appropriate, including any analyses required

by the Information and Privacy Commissioner of Ontario;

(k) Any reports and documentation used in the evaluation of AI technology;

(l) A mitigation plan to mitigate the risks posed by the implementation of the AI

technology;

(m)The estimated cost of acquiring and implementing the AI technology, and any

additional costs or savings expected from the implementation of the AI

technology; and,

(n) Proposed indicators that will be tracked by the Chief of Police until at least 12

months after full deployment of the new AI technology to determine whether the

AI technology is achieving its intended goal and whether its deployment has had

any unintended consequences;

(o) All data and the AI tools themselves must be physically located within the municipal boundaries of the City of Toronto. The technology staff designing, developing, maintaining and supporting the procured toolset must be Canadian citizens with appropriate security clearance, as defined by existing policies and procedures. Additionally the AI tools should ensure that the data doesn’t leave the physical boundaries of the City of Toronto unless approved by an inquiry board of civilians, selected in the same process as juror selection). The purpose of this is to prevent the very sensitive data on people living in Toronto from falling into the wrong hands. (Edit 4)

6. Will not procure, utilize or deploy any new AI technology deemed to be of high or

medium risk before obtaining the Board’s approval;

7. Will inform the Board, at the earliest possible time, of the decision to procure, utilize or

deploy a new AI technology deemed to be of low risk, and explain why the AI technology

was ascribed this risk level; and

8. Will develop and implement a public engagement strategy, commensurate with the risk

level assigned to the new AI technology, to transparently inform the public of the use of

the new AI technology that collects data about members of the public or assists Service

Members in identifying, categorizing, prioritizing or otherwise making decisions

pertaining to members of the public, prior to its deployment.

It is further the policy of the Board that:

9. The Board will review the reports submitted in accordance with section 5 and determine

whether the Service may initiate the procurement, deployment or use of the new AI

technology, and whether any additional analysis, monitoring, auditing and reporting

requirements beyond the ones required by this Policy are to be imposed.

### Monitoring and Reporting

It is the policy of the Board that the Chief of Police:

10. Will monitor from the initiation of deployment and until 12 months after full deployment

of the new AI technology deemed to be of high or medium risk the indicators approved

by the Board under Section 5(n);

11. Will report to the Board, within 15 months of full deployment of a new AI technology

deemed to be of high or medium risk, with such reporting describing :

(a) How the AI technology has generally been deployed or utilized within the first

period until 12 months from full deployment, including with respect to

compliance with applicable privacy laws and other legislative and legal

requirements;

(b) The performance as measured by the indicators approved by the Board under

Section 5(n) of this Policy;

(c) What concerns the Chief of Police has seen raised by members of the public or

Service Members, and how the Chief has acted to address those concerns;

(d) For AI technology deemed to be of high risk, the results of a post-deployment

public consultation on the impacts of the deployment; and,

(e) Whether the Chief intends to continue using the AI technology in the same

manner or in a different manner in the future; and

12. Will continue to track the indicators approved by the Board under section 5(m)5(n) until

it is determined by the Board that no additional monitoring is required.

It is also the policy of the Board that:

13. The Executive Director shall create a method for members of the public to submit

concerns pertaining to AI technologies used by the Service through the Board’s website,

and

(a) Where concerns are expressed with regard to an AI technology deemed to be of

Medium or High risk, for which the Service has not yet submitted the report

required by section 11, will append a summary of the concerns to the report

when it is brought before the Board; or

(b) Where concerns are expressed with regards to an AI technology for which the

Service has already submitted the report required by section 11, or with regards

to an AI technology deemed to be of Low or Minimal risk, will:

i. If the Executive Director finds that the concern raised likely demonstrates

that an AI technology was erroneously assessed as of a lower risk level

than appropriate in accordance with section 1(c), will report on the nature

of the concern to the Board at the earliest possible opportunity; and

ii. Otherwise, report annually to the Board with a summary of the concerns

raised by members of the public; and

(c) Where a communication from a member of the public amounts to a complaint,

will advise the individual or their right to file a complaint with the Office of the

Independent Police Review Director or successor role, or forward the

communication to the Chief of Police, as appropriate, and inform the complainant

of this action; and

14. The Board will review the reports provided in accordance with above section 11 and

determine whether the Service may continue to use the AI technology in question, and

whether any additional analysis, monitoring, auditing and reporting requirements are to

be imposed.

15. That the Board on a monthly basis review who has seen data or AI recommendations and whether they were authorized to do so. If unauthorized, appropriate disciplinary measures should be taken. The only authorized individuals should be those that need to see the data to maintain the technology (ie troubleshooting), or individuals with a court order, or law enforcement officers. However, individual citizens should be able to easily see all data and recommendations the AI toolsets have collected on themselves only. Therefore any AI tool procured/developed by the Toronto police should include an online portal that citizens (either free or incarcerated) can easily use to see what information or conclusions the tool has collected about them. This portal should be governed by privacy standards. If a citizen wishes information collected on them removed from the AI toolset, or wishes to challenge a conclusion, a low cost process must be in place for a judge to review and decide. (Edit 5)

16. Data retention policies must be built around classification of data. General data and recommendations collected by the toolset and not flagged as potentially criminal should be deleted within five days. Data or recommendations flagged as criminal, or potentially inciting violence should be set aside for a period of one month to be reviewed by a panel of judges, who will decide whether the data is relevant and should be kept for investigative purposes, or irrelevant and should be discarded. (Edit 6)

17. That a panel of randomly selected twenty citizens, who are not currently serving in public office or in any law enforcement organization and have not committed a criminal offence within the last five years, review the usage of AI and affirm on an annual basis that the AI toolset has not been used to infringe upon freedom of expression, and that there were no potential violations of privacy. (Edit 7)

### Continuous Review

It is also the policy of the Board that the Chief of Police:

15. Will post on the Service’s website no later than December 2024, and maintain up to date,

a list of all AI technologies currently in use by the Service that are deemed to be of High,

Medium or Low risk, including the following information:

(a) For AI technologies deemed to be of high or medium risk:

i. Name and manufacturer/developer,

ii. Purpose of the technology,

iii. How the technology is used by the Service,

iv. What information is collected by the technology, and

v. What persons or under what circumstances can the technology be

expected to be used;

(b) For AI technologies deemed to be of low risk:

i. Name and manufacturer/developer, and

ii. A brief description of the type of technology (e.g., speech-to-text);

16. Will terminate the use, immediately upon identification, and no later than December

2024, of any AI technology in use by the Service prior to the adoption of this Policy, which

is deemed to be of Extreme risk, and inform the Board of this action with a description of

the AI technology that was identified and the reason that it was deemed to be of Extreme

risk;

17. Will report to the Board, as soon as it is identified and no later than December 2024, of

any AI technology in use by the Service prior to the adoption of this Policy, which is

deemed to be of High or Medium risk, including:

(a) the reason that the AI technology was deemed to be of this risk level, and

(b) a plan to evaluate the risk and any potential harms resulting from the use of the

AI technology, develop a mitigation plan, and seek the approval of the Board for

the continued use of this AI technology;

18. Will review at least once every five years the continued use of any AI technology deemed

to be of High or Medium risk based on:

(a) the quality of the AI technology, its outputs, and associated Key Performance

Indicators; and

(b) the continued need for the use of the AI technology; and

19. Will review at least once every five years the use of any AI technology deemed to be of

High, Medium or Low risk to ensure that the AI technology has not been put to use for a

novel purpose or in novel circumstances that may substantially change the data collected

or used, in a manner that would constitute a new AI technology, or the risk level of the AI

technology,, and, where it is found that an AI technology has been put to a new use in

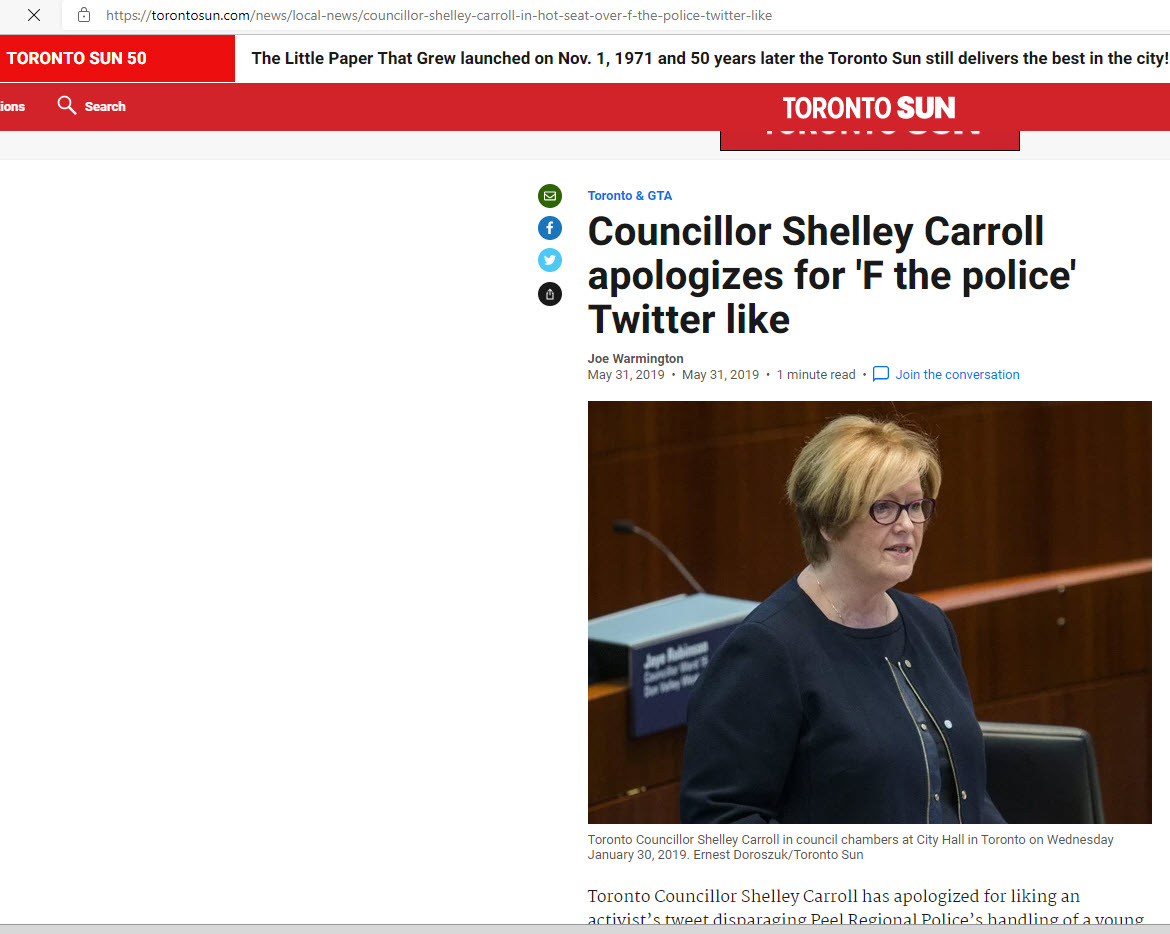
this manner, will report to the Board as soon as possible, in accordance with section 5.

# Justification for edits

## Edits 1, 2

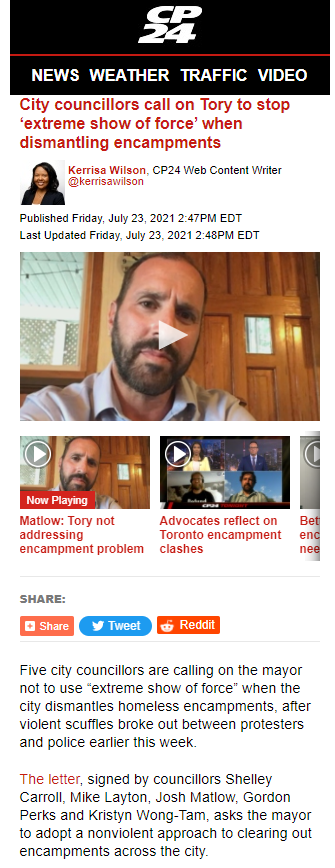
Oftentimes when people are angry they may say things they regret, such as profanities, which do NOT indicate a threat. An inquiry board should review all data pulled from an AI toolset for prosecution/defense to ensure that people’s right to freedom of expression, be it to express frustration at politicians in profanities, or express political viewpoints not in line with the mainstream media, are not submitted as evidence, nor kept in the system. If politicians don’t appreciate the opinions of their constituents, they may exercise their right to freedom of expression by ignoring their constituents (which they almost always do). For example, the tool should not be used to focus on people with political viewpoints such as:

<https://torontosun.com/news/local-news/councillor-shelley-carroll-in-hot-seat-over-f-the-police-twitter-like>



<http://www.genuinewitty.com/2016/10/20/toronto-police-board-member-caught-tweeting-while-driving-feat-shelley-carroll/>

<https://www.cp24.com/mobile/news/city-councillors-call-on-tory-to-stop-extreme-show-of-force-when-dismantling-encampments-1.5521002?cache=yes%2F7.299111>



<http://www.genuinewitty.com/2016/03/20/toronto-police-board-member-promotes-blacklivesmatter-protest-against-siu-decision/>

*One of the earliest mentions of today’s protest came from Alex Hundert, a man convicted and sentenced to 17 months in prison for his part organizing the violence during the 2010 G20- and counseling Ontario youth to commit the violent crime of de-arresting people from police custody. Hundert was arrested with his then girlfriend Leah Henderson, she was sentenced to over a year in prison after telling the judge she “doesn’t believe” in the validity of Canada’s legal system.*

*Despite the fact she’s never publicly apologized, Henderson was later rewarded with a job as city councilor Shelley Carroll’s assistant. Despite several attempts asking for comment, Carroll has yet to have publicly explained her decision to hire an unrepentant ex-con. Henderson has been organizing with and conducting fundraising activities for BLMT. She reported herself being “so fucking proud” of last year’s roadblock*.



As you can see from the above, there has been a consistent stream of anti-police statements from city council, plus city councillors hiring people that use disgusting language in their social media posts, but none are threatening physical harm. This is freedom of expression and the AI toolset should not retain such information, nor draw conclusions from it.

Likewise, if angry constituents state profanities like f—k city council, the AI system should overlook. Politicians should not have special rights, and the AI system must treat them like the rest. Also likewise, politicians who reiterate political viewpoints of the time should not be judged for them within the AI tools, nor should citizens who reiterate the same or opposing viewpoints. Freedom of expression means we can say things to each other that we don’t like nor appreciate, so long as these statements do not constitute a threat to physical harm.

## Edit 3

Calling out specific identity classes already protected by the constitution and existing laws will only have the unintended effect of an AI toolset being tweaked to focus on population groups outside of those aforementioned identity classes; it may lead to a reverse biased system. Just because you don’t get the verdict you want doesn’t mean the system is flawed; the justice system is blind and the presumption of innocence is enshrined into the constitution.

## Edit 4

Data collected regarding crime in Toronto is only relevant to Toronto and there is no need for it to leave Toronto municipal boundaries, unless the RCMP or OPP require it to further their own investigations. In which case they can make a court subpoena for the required data or AI conclusions.

## Edit 5, 7

These are to prevent politicians on the Police Services Board from abusing their power to look at sensitive information regarding their constituents or political opponents. Regardless, privacy mandates that information and AI conclusions/recommendations should be on a need to know basis only. The Police Services Board and other committees may view aggregations of data and/or conclusions, but not information revolving around a specific individual, except for themselves. Thus these ensure that the power over AI and policing remains in the hands of the people, and not corrupt politicians who are easily swayed by biased journalism or special interest groups.

## Edit 6

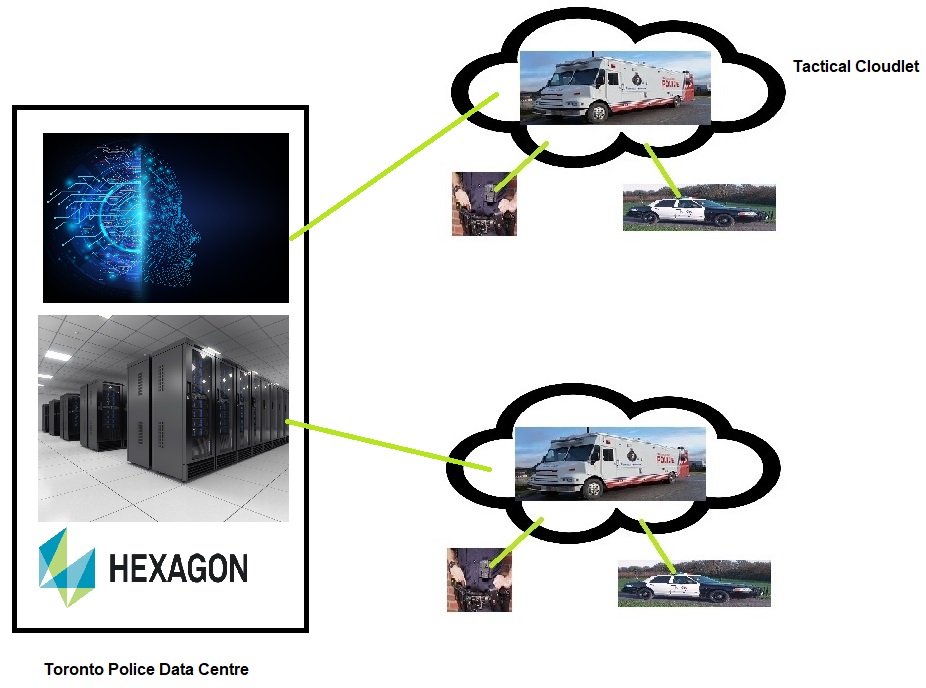
This is a privacy measure as data collected for the purposes of AI should really only be crime focused in this context. If the data is not about a crime or a suspect, then there is no need to keep it as that may infringe upon law abiding citizens’ privacy. Also, given the amount of data that will be flowing in (and required for a reasonably decent machine learning attempt), it is important to keep storage requirements under control otherwise the city will be broke paying for digital storage.

# Potential use cases and their impact on policy

It is difficult to create a policy to govern AI tools without some idea of how they will be leveraged. Therefore, it is important the policy be reviewed and updated periodically. Below are two use cases that would appear to be the most achievable with AI and thus should be considered in policy making first.

## Network centric “responsive” policing

In this model, police sensors and communication devices would be networked electronically and wirelessly to mobile command centers and ultimately, a data center housing tactical data, Hexagon (the dispatch/real-time police locator/etc) system and other tactical systems employed by the Toronto police, such that information from the field would be encrypted and transmitted over air to mobile computing facilities (mobile command centers) to process and reconcile against the full information store in the data center:



Therefore, information police would normally see/hear on a routine patrol, such as random voices, license plates on cars or people’s faces would be encrypted and sent wirelessly to the mobile command unit, which would act as a tactical cloudlet to bring relevant information processing power from the data center closer to the officer in the field, so the AI toolset could more quickly leverage existing algorithmic policing tools (license plate recognition, facial recognition, voice recognition) on a real-time data stream sooner and determine if a stolen vehicle just drove by, or the voice of a wanted suspect was heard nearby, and electronically inform the officer at the appropriate location of the possibility; essentially complete the task of cyber-foraging and provide the updates with less network delay to the end user. Since this information would be things an officer would regularly see while on patrol, this should be acceptable by current privacy policies, but data retention should abide by Edit 6 above. Even though the delay in the AI toolset response may be 30mins, it should be able to provide the officers the direction the suspect is moving. At 30 mins response time, it won’t hurt to have a human operator in the loop to review the AI toolset finding before forwarding to an officer in the field for action, but as newer computer hardware becomes affordable, that response time will shrink.

The above use case should be low tech enough to fit within existing legislation, regulations and policies. Also, given that it is just reacting to daily information to provide a tactical advantage to police in the field, concerns revolving around predictive policing (leading to a focus on marginalized groups) are not relevant in this use case.

The above system could also introduce a crowdsourcing tool that would leverage an app installed on civilian digital devices that they could use to report a crime, feeding into the network centric policing model and hopefully guiding police to violent crimes in progress relatively quickly. This however will require policies around who is allowed to have such an app on their phone and whether they need to go through a criminal background check, etc., before downloading and using said app.

Lastly, the above use case is the necessary first phase in moving to a predictive policing model.

## Leveraging AI tools to anticipate and circumvent organized threats to public safety (Predictive Policing)

This is essentially the use case the US military is considering tactical cloudlets for: to peruse social media and other communication streams for potential coordinated operations orchestrated by non-state actors. Since this would fall under predictive policing, this use case would be the most controversial and likely require many politically influenced policies as governance over the police from over-policing those that like disgusting profanities such as “F--- the police”.

Any such policy enhancements should have a section clearly stating that only groups put on an approved terrorist list as provided by the RCMP, and reviewed by a civilian board, should be accepted. For example, the current government provided list <https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-en.aspx> has Proud Boys on it but the Proud Boys have NO political ambition; they are more anarchists and troublemakers, like ANTIFA. Even Black Lives Matter (BLM <https://legalinsurrection.com/2021/09/report-2020-antifa-blm-led-riots-injured-more-police-officers-caused-more-damage-and-resulted-in-more-arrests-than-the-capitol-riot/>, <https://townhall.com/tipsheet/katiepavlich/2020/09/08/new-study-shows-majority-of-blm-protests-turned-violent-n2575801>, <https://www.dailymail.co.uk/news/article-10233565/BLM-activist-says-Waukesha-Christmas-parade-horror-left-five-dead-linked-Rittenhouse-verdict.html> ) is more a terror group as they are using violence and riots to push a political agenda of undermining the police, who enforce laws legislated by officials democratically elected by law abiding citizens, and BLM has an official organizational structure. It is also surprising entities like the RSS and HSS ( <https://trackingterrorism.org/group/rashtriya-swayamsevak-sangh-rss/>, <https://www.hudson.org/research/4575-hinduism-and-terror>, <https://countercurrents.org/2020/09/rss-as-a-terrorist-outfit-evidences-from-its-archives/>, <https://maktoobmedia.com/2021/10/13/speech-hindu-swayamsevak-sangh-a-global-mouthpiece-for-rsss-genocidal-agenda/>, <https://uncommongroundmedia.com/hindu-nationalism-hindutva-rising-violence-against-indias-christians/>, <https://icnacsj.org/2019/09/exposing-hindutva-an-ideology-of-hindu-fascism/>) are not on the list since their motives and organization reflect that of al Qaeda and ISIS, islamist terror groups already on the list. As part of this AI evaluation that terror list needs to be reviewed and updated. Another edge case to consider would be incels, who really have no organizational structure nor political motivation, but are labelled by the media as terrorists for a few homicides committed by obviously the exceptionally deranged and not by an incel organization per se. Such measures would pre-empt the possibility of leveraging predictive policing for enforcing a political agenda.

Of importance in this specific example of predictive policing is the surveillance of social media by AI tools as part of cyber-foraging and the leveraging of information gleamed from social networks to determine gang membership or terrorist affiliation. Machine learning is only as good as the amount of quality information being fed into it, and even than still quite stupid, but this contingency should be addressed by edits 1, 2, 5 and 7. However policies should be expanded to include controls over what type of data can be ingested by the AI tool for what specific purpose. In this case, I think if the police have a person of interest in mind based on a preliminary investigation, then put that data into the AI tool and see what correlations come up. The tool should NOT be used to survey everyone’s social media and guess which one of us may be criminals, as that would undermine the presumption of innocence; using the tool to predict a potential mass attack by a non-state actor is fine as CSIS and the RCMP already do so.

Another challenge of predictive policing is pragmatic: how do you filter out phony information from real information, and how do you prevent organized crime and other non-state actors from confusing the AI tool with floods of fake data? Policies will have to be in place to govern cyber defenses that need to be built around a network centric predictive policing model to ensure its integrity. The easiest thing a non-state actor can do is defeat the predictive policing toolset with volumes of fake data.

# References

<https://citizenlab.ca/2020/09/algorithmic-policing-in-canada-explained/>

<https://www.hexagonsafetyinfrastructure.com/about-us/case-studies/tps-integrates-location-and-navigation-using-mobile-cad>

<https://resources.sei.cmu.edu/asset_files/Webinar/2015_018_101_433376.pdf>

<https://insights.sei.cmu.edu/blog/tactical-cloudlets-moving-cloud-computing-to-the-edge/>