LAW UNION OF ONTARIO
POLICING COMMITTEE

31 PRINCE ARTHUR AVENUE
TORONTO, ONTARIO M5R 1B2
TEL. (416) 964-7406 EXT.153
FAX. (416) 960-5456

SENT BY E-MAIL AND SUBMITTED VIA TPSB PORTAL

December 14, 2021

Dr. Dubi Kanengisser
Senior Advisor, Strategic Analysis and Governance
Toronto Police Services Board
40 College St.
Toronto ON M5G 2J3
dubi.kanengisser@tpsb.ca

Dear sir,

Use of New Artificial Intelligence Technologies Policy - Public Consultation

The Policing Committee of the Law Union of Ontario welcomes this opportunity to provide our feedback about the proposed TPSB AI policy. We commend the TPSB for starting the process for public examination of the enormous impact of new police technologies on our rights and freedoms and on our way of life. There is a crying need for effective institutional governance and regulation in this area through the TPSB and its policies and consultive processes and through the TPS and its procedures. However, we have serious concerns about the consultative process adopted by the TPSB and the draft policy itself.

Overview

To begin with, we think it is a mistake to focus solely on AI as the game changer that needs to be addressed. We acknowledge that AI is currently the technology *du jour*, holding out great potential benefits and posing enormous potential risks. But in the last analysis AI is merely a tool that uses vast quantities of data to develop software solutions to process and characterize new data inputted into it. The real questions are human ones: for what purposes are we developing and using these systems, how do we validate such systems, to what uses do we put the results the AI provides, what are the consequences and risks arising from our use and reliance on such systems, and how does the deployment of these AI applications empower and disempower individuals, sectors and institutions in our society.

We think AI should be viewed in the context of the much larger technological revolution that is transforming policing and its relationship to our society. The last 20 years have seen the widespread use in new policing technologies that range from the relatively mundane, such as laptops in patrol cars and cellphone cameras to record evidence to sophisticated surveillance systems such police-operated or police-accessible surveillance cameras in our public areas, automated license plate recognition systems (LPR), facial recognition technology (FTR), computerized graphic image enhancement (CARES), infrared thermal imaging (such as FLIR),

night vision cameras, and gun shot identification and tracking systems to forensic information systems such as automated fingerprint identification systems (AFIS), integrated DNA databases (CODIS), and digital mugshot systems (RICI), to police management systems such as predictive policing software to database systems involving computerized digital storage systems capable of storing many terabytes of case files, criminal records, surveillance videos, wiretap intercepts and other evidence coupled with sophisticated database management and analysis software. More recent technologies being used include body cameras, camera carrying drones, spyware and other hacking tools for accessing cellphones, and automatic transcription and translation software. Not far off, if not already being used, are automated voice identification systems, sentiment mapping, and advanced video analytic software capable of object and event detection and the automatic monitoring of large networks of surveillance cameras.

AI will undoubtedly offer significant improvements in many of these areas, the most obvious being facial recognition. It will open doors to new applications to process the information obtained through existing and new technologies and present both known and unforeseen challenges.

But the policy should really apply to all intelligence-gathering technologies that could potentially impact the privacy, human rights and *Charter* rights of individuals, not just AI.

Bearing this in mind, the Policing Committee of the Law Union makes the following submissions:

1. *The TPSB and TPS should inform the public about the current use of and plans for software to enable or enhance intelligence gathering and analysis, including facial recognition software, predictive policing software, and automated surveillance systems.*

It is very difficult to have a meaningful consultation process on a policing policy without knowing what the TPS has been doing, is doing and plans to do in this area. Facial recognition software, predictive policing systems and other surveillance and intelligence-based software have been used by police forces in Canada and elsewhere in the world for at least a decade. It would help inform the public debate if we knew which such systems the TPS has used and what its experience has been with them.

Real transparency is required right now. Both the TPSB and the TPS have a history of preaching transparency but then falling back on a longstanding culture of secrecy. The proposed policy is evidence of this. The draft Policy gives the Chief of Police **three years** to publicly post a list of all AI technologies currently in use by the TPS (Section 15). This is both too long and too narrowly drafted. The TPSB should require the Chief to publicly post the details of any intelligence gathering and analysis software currently in use by the TPS, whether AI based, to it by March 1, 2022.

For any High or Medium Risk technology the TPS wishes to use, the Chief should be required to make publicly available the nature of the technology under consideration, its intended uses, its ascribed risk level, the steps proposed to minimize or mitigate against risks, and the risk and privacy assessments carried out for it to enable public input prior to any Board approval.

2. *The TPSB should strike a Technology Review Committee of experts to provide the Board with advice about existing and proposed intelligence gathering and analysis software and systems.*

The Policy should require the TPSB to strike a Technology Review Committee to provide expert advise on the impact of such technologies. Toronto is lucky. It is a world class centre for AI development, innovations and applications. It is the home to government institutions devoted to human rights and privacy, to sophisticated university organizations like the Citizens Lab and to an active bar. It has a long history of civic engagement in policing. The TPSB should take advantage of this fortunate state of affairs by striking a permanent Technology Review Committee to review and provide advice and recommendations on intelligence-gathering and analysis software and their implications for human rights, privacy and criminal prosecutions and on TPSB policy initiatives in this area. AI is a rapidly evolving technology that will need to be continually assessed by experts in the field. The Policy should require the TPSB to consult with its Technology Review Committee before approving the procurement or use of any High or Medium Risk technologies.

As well, the Board should consult with its Technology Review Committee about the draft Policy before adopting it. The Board should have the benefit of the Committee's expertise about what information it needs, what criteria it should consider and what are the appropriate processes that should govern the Board in making its decisions. The Committee should also advise the Board about the known problems with specific technologies, such as facial recognition and predictive policing. The Board should consider these issues before embarking on an *ad hoc* case-by-case approach to the technologies the Chief wishes to procure.

The Policy should also require the TPSB to engage in a public consultation process before approving any High or Medium Risk technology. This is constistent with the principal that the public should have a say in any decision to use technology that will impact the human and *Charter* rights of individuals or have the potential to disadvantage or discriminate against any group in our society subject to OHRC or *Charter* protection.

3. *The TPSB should require that any software used for intelligence gathering and analysis or to guide or further investigations be validated in accordance with industry and government standards before use and that officers using such software be trained as to the appropriate use and limitations of such software.*

The draft Policy creates an unworkable standard for complex software systems including AI-based systems when it deems any system which "cannot be fully explainable in its behaviour" as a High Risk Technology. Virtually all complex software systems cannot be fully explainable in their behaviour. They produce unexpected results and inexplicable glitches and crashes on occasion. Like some facial recognition and predictive policing systems, they may have hidden biases that may not be readily apparent from an examination of their source code and algorithms, which may in theory offer a full explanation of the software's behaviour but in reality do not. In most cases, the source code is unavailable, protected by copyright and end user agreements, making any explanations impossible. How neural net AI systems trained on large datasets work is in fact currently unknown in any detail and their behaviour is unexplainable in any meaningful

sense. A sophisticated neural net AI software system may have created literally millions of parameters in the course of its training to do its job.

More important than knowing how the software works in theory is establishing that it works to an appropriately high level of performance and accuracy. The Policy should require that any High or Medium Risk technology be validated against appropriate and transparent industry, national and international standards, that their limitations and error rate be known, and that they be subject to continual internal review based on results obtained, errors both software and human that have occurred and evolving standards. Software should meet appropriate internal and external security standards to minimize the risk of unauthorized access or use or attempts to "game" the software, whether by external hackers or internal staff. Audit trails should be mandatory.

The Policy should also require the AI software vendor to provide the details of what databases were used to train the program and the source of the data in the databases. This is necessary in order to implement Section 1 (b) i 5 of the draft Policy.

4. *The Policy should address the use of TPS databases and the TPS use of exterior databases for the training and creation of AI software.*

Some of the current AI technologies are very general in application and can use a wide variety of datasets to train the software for specific applications. Large police forces like the TPS are repositories for enormous datasets, ranging from surveillance videos and photos to mugshots to wiretap records. This leads to the prospect of the development of internal AI applications and the creation of police and government consortiums to pool data for development of AI applications. The Policy should apply to these applications, to the acquisition of general AI technologies for creating such applications, to the use of TPS data sets for such purposes, and to the need to control the distribution of such AI applications to third parties.

5. *The Policy should center on the proposed and potential uses of the software and the need to prevent and minimize the chances of misuse.*

The TPSB should exercise its jurisdiction to establish policies about the acceptable purposes and uses of such technologies and about the limitations on their use rather than rely on the Chief to determine this on an *ad hoc* basis for each technology the TPS wants to procure. The purpose for which the technology is to be used can drastically affect its impact of human and civil rights. Policing runs on a continuum of purposes from the investigation of a specific offence or crime to specific intelligence-gathering relating to criminal organizations to general intelligence-gathering such as carding and its equivalents to proactive, preventive or community-based programs. Using facial recognition to try to get an investigative lead from surveillance footage of capturing the image of a shooter is one thing. Using it to identify demonstrators protesting a police shooting is another thing. It is the use and purposes that matter, not so much the characteristics of the technology itself. The consequential uses of the technology are important too. Are the results going to be used to follow a potential suspect, obtain a search warrant or wiretap, or form the grounds for an arrest?

The TPSB should set minimum standards of controls on the use of these technologies. Even an indispensable and seemingly benign technology like CPIC can be misused such as where an officer uses it to run a check on the ex's new partner. One solution is to require audit trails for all of these technologies as is currently done with CPIC. Another solution for more specialized or risky technology is to restrict access to the technology to officers or staff who have been trained in its use and how to interpret the results. The Board should set these standards.

6. We have attached a marked-up copy of the draft Policy with some proposed changes.

The marked up copy of the draft Policy with our comments should be read in conjunction with these submissions.

Thank you for giving us an opportunity to make these submissions which we hope will help the Board in dealing with this important and complex issue.

Yours sincerely,

_____

Jack Gemmell

For the Policing Committee, Law Union of Ontario