HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

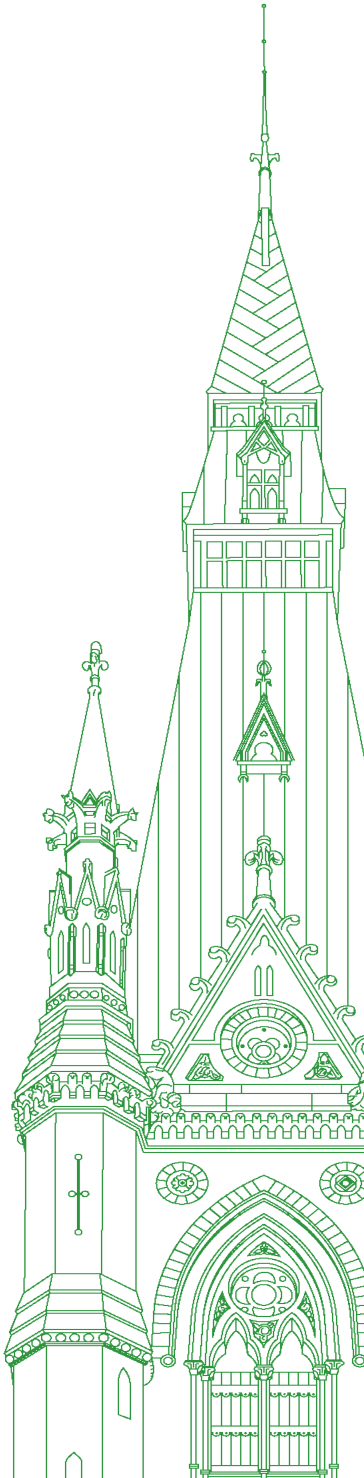
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 017

Thursday, April 28, 2022



Chair: Mr. Pat Kelly

Standing Committee on Access to Information, Privacy and Ethics

Thursday, April 28, 2022

● (1610)

[*English*]

The Chair (Mr. Pat Kelly (Calgary Rocky Ridge, CPC)): I will call this meeting to order.

I will start the meeting by apologizing to our witnesses. This is the time of year where this kind of thing happens more frequently, when we are disrupted sometimes by votes in the chamber. This meeting is late to begin because of a rare Thursday vote and looks like it will be cut short because of another vote.

Thank you to our witnesses.

In the interest of time, each witness here has prepared an opening statement that has been received in writing. I would like to receive those statements for the record to be included in the evidence as read, but dispense with the reading of the statements, so that we may have time, perhaps, for a full round of questions from parliamentarians.

[*See appendix*—Remarks by Paul Boudreau]

[*See appendix*—Remarks by Dubi Kanengisser]

The Chair: Greg, I see your hand up. Go ahead.

Hon. Greg Fergus (Hull—Aylmer, Lib.): I know this is on me. I had not read the witnesses' statements before the meeting. I actually would appreciate hearing them give their statements, sir.

The Chair: You likely won't get to ask any questions if we simply have statements read. Time allocation's been moved in the chamber and we're expecting bells to go probably in about 20 minutes or so.

My proposal is that if I end up with unanimous consent to take us partially into the period of bells, we may get a round of questions in with our witnesses. I want to devote about three or four minutes tops to deal with some important committee business that can't wait.

Greg, go ahead.

Hon. Greg Fergus: Given what you've just told us, sir, are we going to be coming back after bells?

The Chair: I think we'll be past 5:30 by the time we get back. That would be my guess.

Matthew.

Mr. Matthew Green (Hamilton Centre, NDP): Thank you, Mr. Chair.

I have a pretty significant concern that we're going to lose this portion of the study. I know that we had spoken about the potential for additional witnesses. This is an occupational hazard. This has happened from time to time, but I don't want to gloss over this very important element, given the impact it has on our communities.

Through you, Mr. Chair, to our clerks, I'm just wondering whether there are opportunities to invite these witnesses back to have a full discussion? Do we get a mulligan on this?

The Chair: I don't think I'm in a position to answer that question.

We have a lot of moving parts with our committee. We may have time for another meeting where perhaps they could be reinvited. This is going to take up their time as well. We're at quarter after four. My proposal really is to give a member from each party six minutes and see where that takes us. We're likely going to be into bells by the time we do that. I'd like to go ahead and maybe give the floor to our first round and go from there.

Iqra.

● (1615)

Ms. Iqra Khalid (Mississauga—Erin Mills, Lib.): Thanks, Chair.

Again, we wouldn't really have context for the questions we want to ask if we don't hear opening statements. I would humbly suggest that maybe we get two minutes per witness just to give them an opportunity to highlight what is really important to them and then move on to the questions.

I would really appreciate that, Chair.

The Chair: I'm going to suggest that you have the latitude to use your time however you wish and turn it over for part of that.

There was a briefing note prepared by the analysts as well that maybe you can refer to for questions if that's what you'd like to do. I'm just trying to use our time as effectively for members and ensure that members have an opportunity because otherwise you won't.

With that, I'm going to go ahead.

Mr. Williams, you have six minutes.

Mr. Ryan Williams (Bay of Quinte, CPC): Thank you, Mr. Chair.

Thank you to all the witnesses for coming today.

I really want to focus testimony today on the facial recognition technology. We've had witnesses in the past who've identified that this technology is wildly inaccurate in identifying non-white individuals.

Can you please just share with me how you're using that technology right now? Are you aware of that inaccuracy in terms of its use and how you're using it?

I'll start with whoever wants to answer that.

Mr. Paul Boudreau (Acting Deputy Commissioner, Specialized Policing Services, Royal Canadian Mounted Police): When it comes to technology such as facial recognition, we recognize that there are gaps in the technology. There are biases that are inherent to those types of technologies.

What we're doing, from an RCMP perspective, is when we look at these new technologies, whether they be facial recognition or other types of technologies, we're looking at processes to include human intervention to assess any of these new technologies—

The Chair: If I may, the witness's camera is not engaged.

Mr. Paul Boudreau: I apologize for that.

Whenever you look at these types of technologies, you have to look at them through the lens of a legal, privacy, gender-based analysis and bias perspective. As I mentioned, you have to have that human intervention as well.

There are gaps in these technologies that we must assess. We must make sure that when they're used, they're used properly—especially from my perspective—from a law enforcement perspective.

Mr. Ryan Williams: Right now, are we using human intervention or human review with this technology, as it stands?

Mr. Paul Boudreau: The RCMP is not using facial recognition technology, as it stands. When we used it as part of our Clearview licences, there was human intervention every time there were results returned by the Clearview application. Yes, we absolutely required human intervention.

Mr. Ryan Williams: I'll go to Mr. Stairs from the Toronto Police Service. Is the Toronto Police Service using facial recognition technology right now?

Mr. Colin Stairs (Chief Information Officer, Toronto Police Service): We are. We're using facial recognition to compare probe photos that would have been uncovered in investigation against our Intellibook, which is our mug shot database.

There is a known set of issues around faces in different training sets. We selected the facial recognition technology we use because it is the least biased, but there are biases that are embedded into photography and the photographic systems that are out there. There are biases towards lighter faces, and having more of a detail range in lighter faces than in darker faces.

What we're doing is countering that bias by having a hurdle rate below which we don't consider it a match. If the technology is weaker, it does not disfavour the generally racialized minorities who have darker skin tones. We're also feeding that into a process whereby a match is not considered an identity. The identity has to be corroborated by other methods.

● (1620)

Mr. Ryan Williams: Is that human intervention that you're using? What are the other methods? If you're misidentifying a racial minority, who's verifying that data?

Mr. Colin Stairs: It would be through the investigative processes.

Mr. Ryan Williams: Is that human?

Mr. Colin Stairs: Yes, definitely.

Mr. Ryan Williams: In terms of the data you're collecting from FRT, are you having human intervention every time, or is there sometimes not any?

Mr. Colin Stairs: There's never no human intervention. There will always be a human intervention.

Mr. Ryan Williams: Almost every witness who's appeared before this committee—academics, lawyers and civil liberties experts—has called for a moratorium on the use of FRT by police forces. Are you aware of the support for moratoriums?

Mr. Colin Stairs: I am aware, yes.

Mr. Ryan Williams: At this point are you considering that, or is that something that should be happening at the police force until this technology is examined further?

Mr. Colin Stairs: I don't believe so.

This is how we've approached this with our AI/ML policies. There's a balance of goods around this. There's a social good around public security and safety against privacy and human rights challenges with the technology.

The question is, when do we deploy this technology? For us, it's only in major crimes and major cases. We're not using this technology broadly. We're using it where there's a significant benefit to public safety around the identification of individuals who are involved in violent crime.

Mr. Ryan Williams: Thank you.

Mr. Boudreau again, the Privacy Commissioner said that the database of faces that Clearview AI created for the RCMP was an illegal compilation and violated the Privacy Act.

Has the member of the RCMP who authorized this illegal activity been reprimanded in any way?

Mr. Paul Boudreau: No. If we look at the results of the Office of the Privacy Commissioner and what the commissioner stated, we do not agree with the full findings of the Privacy Commissioner. However, we do fully support all of the guidance that's been provided and recommendations to the organization.

The RCMP has stood up, since the report, a new program called the national technology onboarding program that looks at all new technologies from a legal, ethical and privacy perspective. It's not just facial recognition, but any new technology that may have privacy or legal implications.

The RCMP believes that the use of facial recognition must be targeted, time-limited and subject to verification by trained experts. Further, facial recognition should not be used to confirm an identity, but rather only be considered as an investigational aid where the results must be confirmed, again, by human intervention.

The Chair: Thank you.

That's good for the first six-minute round.

Mr. Fergus, you have six minutes. Go ahead.

[*Translation*]

Hon. Greg Fergus: Thank you, Mr. Chair.

I'd like to jump in and pick up on a question that Mr. Williams just asked.

Mr. Boudreau, you responded that the RCMP no longer uses facial recognition in its operations. Can you confirm that this is the case?

[*English*]

Mr. Paul Boudreau: Yes. If you look at the technologies such as Clearview AI, you see that the RCMP is not using any new or advanced facial recognition technologies. The RCMP inherently has used facial recognition as part of our processes in the past. We can look at mug shots and those types of activities, but facial recognition technology, per se, we are not.... As part of the review from the Office of the Privacy Commissioner, we did an exhaustive survey across the organization to try to discover any new facial recognition technologies that are being used. We provided those results to the Office of the Privacy Commissioner to—

[*Translation*]

Hon. Greg Fergus: Mr. Boudreau, I apologize for interrupting you. Your answer seemed quite categorical, but I'm thinking about the Project Arachnid platform, which uses a form of facial recognition to identify victims of child pornography. Is this true or am I wrong?

● (1625)

[*English*]

Mr. Paul Boudreau: Yes. Project Arachnid actually runs out of the C3P program, not out of the RCMP. They do use facial recognition technology. We do work with partners such as C3P with regard to child exploitation, but that is not an RCMP-led activity.

[*Translation*]

Hon. Greg Fergus: That raises another question, Mr. Boudreau. Are there any other RCMP partners using facial recognition?

[*English*]

Mr. Paul Boudreau: There may be. I am not aware of other technologies out there. The one with Project Arachnid is significant because of its profile dealing with child sexual exploitation, and we have a strong working relationship with C3P. Outside of that, I am not aware of other technologies being used by the organization.

[*Translation*]

Hon. Greg Fergus: Mr. Boudreau, could you please check with your colleagues, list all your partners who use facial recognition, and provide that information in writing to the clerk of our committee?

[*English*]

Mr. Paul Boudreau: Yes, that can be achieved.

[*Translation*]

Hon. Greg Fergus: Thank you, Mr. Boudreau.

[*English*]

My next question would be for the Toronto Police Service and whoever would like to answer this question.

Again, in a similar sentiment to Mr. Williams, I'd like to know if you could provide us in writing—if they exist—the policies that you use to determine when you would or would not use facial recognition technologies. Would that be possible, or would you be able to give me a quick, one-minute summary in terms of some of the guiding principles that you use?

Dr. Dubi Kanengisser (Senior Advisor, Strategic Analysis and Governance, Toronto Police Services Board): Mr. Chair, I could respond to that.

Along with my opening remarks, I also submitted the Toronto Police Services Board's recently approved policy on the use of AI. That also encompasses any use of facial recognition. Anything that uses facial recognition or other biometrics is considered high-risk technology and therefore will require considerable reviews in advance of adoption and deployment, and a follow-up over at least two years to examine any impact, including any unintended consequences.

You should have a copy of that with you. It details all the different aspects that are looked into, the concerns and the guiding principles in deciding whether or not a certain technology may or may not be approved. That includes issues of fairness and reliability and the legality of that use, as well as the requirement that there always be a human in the loop, and personal and organizational accountability for its use.

Hon. Greg Fergus: I see that Mr. Stairs has an additional comment to make on that, but I'd like to ask a question to both of you because my time is running down.

We all recognize, it seems to me today, the limitations of this technology. What recourse does the public have to ensure that their images are indeed...especially for members of the community and people of colour? What are their rights in terms of how you assess the efficacy of the use of facial recognition technologies?

Mr. Colin Stairs: I'm just going to respond to the first question.

We can supply the Forensic Identification Services policy on facial recognition and what qualifies for that. There's a fairly stringent set of criteria, and we can supply those separately.

In terms of rights, we're operating under the Identification of Criminals Act, so we're only using images from mug shots, essentially from arrests and processing, and so there is no use.... Obviously, Clearview was a blip in that. There is no use of publicly sourced facial images for our facial recognition program.

● (1630)

The Chair: Thank you.

A voice: If I may add to that, Mr. Chair?

The Chair: We're considerably over Mr. Fergus' time, so I'm going to have to go next to Mr. Villemure.

[*Translation*]

Mr. Villemure, you have the floor for six minutes.

Mr. René Villemure (Trois-Rivières, BQ): Thank you, Mr. Chair.

Mr. Kanengisser, could you briefly weigh up the pros and cons of the use of facial recognition, from the point of view of the freedoms concerned?

[*English*]

Dr. Dubi Kanengisser: Thank you.

Mr. Chair, through you, it's hard to discuss very broadly the issue of facial recognition without the context of the particular use. There are definitely many concerns that you've heard throughout these discussions. There is also the obvious benefit of successfully cracking cases and identifying victims and rescuing them in cases of abuse. I don't think I can give a clear answer without a specific context.

The policy the board approved recently was really setting the groundwork for having these discussions and requiring the service to provide a business case, basically, and a justification that would prove they are effectively balancing the risks with the benefits and are mitigating those risks in a way that minimizes any kinds of impacts on privacy and freedoms.

[*Translation*]

Mr. René Villemure: Of course, we recognize that there are advantages and disadvantages.

What came out of the public consultations you held recently? What were the concerns of participants?

[*English*]

Dr. Dubi Kanengisser: There were two kinds of concerns. Well, there are a few concerns, but I think the greatest ones had to do, as we've discussed here earlier, with the misidentification of individuals and also from the contrary side where the technology is effective with basically mass surveillance and unreasonable levels of surveillance over people just going about their business. Both of these concerns were important. The ability of a person to go around town and not be followed around using artificial intelligence and facial recognition technologies is something that we are concerned about, and this is something that will be prevented through our policy.

[*Translation*]

Mr. René Villemure: Is the use of facial recognition more about increasing security, or a feeling of security?

[*English*]

Dr. Dubi Kanengisser: Through the chair, I think neither of these will be the correct answer. It's supposed to help law enforcement identify perpetrators and victims, to help them carry out their duties. So whatever duty that you believe that law enforcement has, it is just another tool in their belt to carry out those duties. I don't think the expectation is that actual safety, or a sense of safety, will be impacted directly just by having those tools available.

[*Translation*]

Mr. René Villemure: Thank you, Mr. Kanengisser.

Mr. Stairs, I'll ask you the same question: can you weigh up the pros and cons, from the point of view of personal freedoms?

[*English*]

Mr. Colin Stairs: I agree that what we're looking at is mostly an after-the-fact investigative tool, and we are not looking at surveillance or upstream of event types of facial recognition, which would be very intrusive. And in that state, I don't think we're having a significant impact as it stands on rights because we are following similar processes at similar scales to existing processes.

I think that when the public thinks of facial recognition, they think of TV shows and movies where every camera has facial recognition applied to it. What we are doing is taking crime scene photos gathered from cameras that would be recording the street regardless, taking a still from that and comparing it to the mug shot database, which is very similar to witnesses giving testimony. This is not a significant change.

● (1635)

[*Translation*]

Mr. René Villemure: Thank you very much, Mr. Stairs.

I'll get back to Mr. Kanengisser.

What uses of facial recognition technology would you call unreasonable?

[*English*]

Dr. Dubi Kanengisser: Anything that falls under mass surveillance would definitely be unreasonable. Tracking people en masse indiscriminately would be considered unacceptable to me and to the board based on their decisions, as well as any use of technology that can be shown to be inaccurate, leading to significant misidentification and all the harm that that could lead to. A person getting arrested because they were misidentified by a software and that wasn't confirmed by a human would be unacceptable.

[*Translation*]

Mr. René Villemure: I'm only going to take 10 seconds to ask you whether or not the people who participated in the public consultation had confidence in the process.

[*English*]

Dr. Dubi Kanengisser: Some did, some didn't. I'm afraid that's the way these things go. Conversations that I've had with—

The Chair: I'm going to have to leave the answer at that.

It is time now for Mr. Green, for six minutes.

Mr. Matthew Green: Mr. Boudreau, I heard you state in earlier testimony under questions from Mr. Williams that you didn't agree with the Privacy Commissioner's results and findings, and in fact, if I believe I understood correctly, there was no disciplinary process through which those responsible for this breach were held to account. Is that correct?

Mr. Paul Boudreau: That is correct, and the RCMP appreciates the—

Mr. Matthew Green: Mr. Chair, Under the RCMP Act, if an officer were to unlawfully access CPIC, for instance, to look at information relating to people unrelated to a crime, what would happen under the RCMP Act in terms of disciplinary processes?

The Chair: Before we get an answer to that question, I'm obliged to interrupt at this point and ensure that I have unanimous consent.

I'd like to hopefully finish Mr. Green's round, and I have a couple of very quick items that could probably be dispatched within a minute or two.

If there are no further objections, I will go to the answer to Mr. Green's question.

Hearing none, we'll continue to finish Mr. Green's round and a couple of other quick items.

Go ahead for the answer.

Mr. Paul Boudreau: If the RCMP breaches a code of conduct in which having access to information is used improperly, we would go through the conduct process, which may or may not—

Mr. Matthew Green: Why was this process not undertaken when the person was found to have unlawfully accessed these without knowledge of superiors?

Mr. Paul Boudreau: Again, the RCMP is in disagreement with the Privacy Commissioner in regard to its findings, in particular with section 4 of the Privacy Act.

Mr. Matthew Green: Mr. Chair, the OPC report also states that the RCMP first erroneously told the Office of the Privacy Commissioner that it was not using Clearview AI. Why did the RCMP deny the use of the technology to the Office of the Privacy Commissioner?

Mr. Paul Boudreau: At the beginning, when we initially responded to media inquiries, to the Privacy Commissioner, it was not commonly known across the large organization of the RCMP that a limited number of programs and services had begun to use Clearview AI.

When it did come to our attention, the RCMP did a fulsome survey to discover how this technology was used across the organization, at which point we instilled processes and procedures on the use—

Mr. Matthew Green: At the highest level of accountability, who would have allowed for this and signed off on this use, whether in a procurement process or in free trials? Who ultimately signed off on the use of this technology? It sounds like the superior officers were unaware of this, so who ultimately is responsible?

Mr. Paul Boudreau: The RCMP constantly looks at new and emerging technologies. It's part of our processes for which the divisions—we have a very large organization—look at and evaluate new technologies. What we've done to capture these activities is that we've created a new process called the national technology—

● (1640)

Mr. Matthew Green: Mr. Chair—

The Chair: Let him answer, because he's—

Mr. Matthew Green: I'm not actually interested in what they're doing now. I'm interested in what happened to get us to this point.

The Chair: I just want to make sure he has enough time to answer the question. It was a 25-second question. I was just letting him answer.

Mr. Matthew Green: Let me ask a more specific question, Mr. Chair.

In earlier testimony from Mr. Williams and others, I heard that FRT was not used per se. Why per se? I also heard that no new or advanced AI technologies were being used.

My question is, through you to Mr. Boudreau, are any forms of FRT, either old, or not considered new and advanced AI, being used currently by the RCMP?

Mr. Paul Boudreau: As mentioned earlier, I think facial recognition technology is very large, and I think we need to look at it as new technology. We've been using facial recognition within the organization for a very long time.

When it comes to the use of facial recognition technology such as Clearview, we are not using that type of technology.

Mr. Matthew Green: What about other types of technology, Mr. Chair?

Mr. Paul Boudreau: I am not aware of any other types that would fit the same bill as facial recognition technology. We also shared this information with the Office of the Privacy Commissioner after confirming its use within the organization.

Mr. Matthew Green: Mr. Chair, we heard testimony from the RCMP that this was to be used for things like crime scenes, and not as though we would see it on television with every camera having access to this. Is the RCMP using this for the active surveillance and capturing of mass protests?

Mr. Paul Boudreau: No, it is not.

Mr. Matthew Green: Thank you.

Mr. Chair, I will go on to the Toronto Police Service.

In my time as a city councillor, I fought vigorously against the practice that I consider to be racist in street checks and carding—racial profiling, essentially. How is the Toronto Police Service's use of this technology not simply a more advanced and highly technical version of the same practice?

Mr. Colin Stairs: Mr. Chair, the street-check practice is discontinued, but that is a practice—

Mr. Matthew Green: You don't need it now. Is that not correct? There's no longer the need to stop and ask for information when you can simply take a photo and run it through facial recognition technology.

Having been involved in direct action in my own city, I know that our local police are constantly there and consistently there taking photos of protesters. Does the Toronto Police Service also do the same practice? Do they run those photos through any AI technologies?

Mr. Colin Stairs: We do not.

Mr. Matthew Green: Thank you.

Mr. Chair, with my remaining minute, I just want to note that we are in what I think is the crux of much of the discussions we have around civil liberties. Pertaining to these witnesses, I would like to formally request that this committee consider extending this study for a day to have these members come back, because there is a line of questioning that I think deserves further depth.

Given the fact that we're going to be called back to the House, I want to make sure that these gentlemen here have the ability to fully testify under this committee's study.

The Chair: That is noted. We'll have to assess our calendar. I appreciate the importance of these witnesses. I believe we have time for two more meetings on this study. There are other competing witnesses, though, that other parties have requested, so I'll take that under—

Mr. Matthew Green: I would also be happy to suggest, Mr. Chair, that if they were to come back along with other witnesses, we might be able to better fully examine the use.

The Chair: That is noted. I will do my best to accommodate that, but we are constrained by the calendar. I'll take that under advisement, certainly.

With that, we are—

Mr. Damien Kurek (Battle River—Crowfoot, CPC): I have a point of order.

The Chair: Okay—a quick one, if you may, please.

● (1645)

Mr. Damien Kurek: I would just note, Mr. Chair, that if the witnesses have further information to submit beyond their opening statements, or if they have interest in expanding on some of their answers, they are welcome to submit that information to the clerk and it will be distributed to the committee.

The Chair: Indeed the witnesses may do that.

I will note that until statements are translated, they can't be distributed to members. The members in some cases were not privy to all of the opening statements that we received, even though they were submitted. They are not distributed to members until they are translated.

I thank our witnesses for coming today. I'm sorry that this meeting...but activity in the House always takes priority. When votes happen in the House, we have to vote.

With that, I'll thank the witnesses for attending. They may leave the call.

I would ask members to just give me a minute.

First of all, I would ask the committee for a motion to approve the budget for this study, which was circulated.

Hon. Greg Fergus: I so move.

The Chair: Mr. Kurek, go ahead.

Mr. Damien Kurek: On a point of order, Mr. Chair, I would just note that in my examination of the budget, and understanding the good work that our translators do, I'd certainly value an explanation as to why each headset is being charged at a cost of $175. That seems a lot.

I don't want to hold up the work. I understand that our translators do good work. I'll leave it at that.

The Chair: I think that will be a question maybe better put at liaison committee—

An hon. member: OGGO.

The Chair: —if you really want to go there.

Is there any further discussion on the budget?

All those in favour of the budget as distributed?

(Motion agreed to [*See Minutes of Proceedings*])

The Chair: There is one last thing I will remark on before we go to the vote. There was a draft first plan distributed to committee members for the travel proposal, as per the motion by Monsieur Villemure.

If anybody has any comments on that, or concerns or objections, perhaps I would invite you, if there are any, to—

Hon. Greg Fergus: So moved.

The Chair: All right.

Mr. Fergus has moved the adoption of the report as circulated.

All those in favour of the proposal that was circulated?

(Motion agreed to [*See Minutes of Proceedings*])

The Chair: With that, the meeting is adjourned.

Dubi Kanengisser – Opening Remarks

Thank you for inviting me to speak before the committee. My name is Dubi Kanengisser, I am a senior advisor, strategic analysis and governance to the Toronto Police Services Board (TPSB), and I led the development of the recently approved Board Policy on use of artificial intelligence by the Toronto Police Service, which is, to the best of our knowledge, the first of its kind in Canada.

Before I begin I would like to clarify that I am not speaking today on behalf of the Board. I encourage you to refer to the Minute that I have submitted with the attached Board Report, as approved by the Board in February 2022.

The TPSB's Policy on the Use of Artificial Intelligence Technology was developed to guide future discussions on particular AI implementations that the Toronto Police Service (TPS) may seek to use. The Policy sets the requirements for the evaluation and analysis of any AI tools, and the requirements for Board approval, prior to their adoption. These requirements are risk-based, based on a scale from minimal-risk tools that are internal only and are not likely to impact any individual's rights or freedoms, up to extreme-risk tools which are completely prohibited.

Along this scale, the Board's Policy identifies any AI tools that make use of biometrics to identify individuals, as high-risk. Categorizing these tools as high risk leaves the door open for the TPS to bring forward a business case for the adoption of such tools, provided that they successfully demonstrate that it responds to a real operational need, as well as its accuracy and fairness, and provided that they present a mitigation plan to address any risks of bias or infringement of privacy or other rights. The Service will also have to ensure a governance structure that would allow for the effective auditing of any such tools, and report on outcomes, including possible unintended consequences.

An important challenge that we faced in developing this Policy has to do with the training necessary for Service members, both officers and civilians, to even recognize that a tool uses AI, and may therefore pose risks that may not be immediately evident. AI is incorporated into many easily available apps that anyone could install on their phone and use. Police officers are resourceful people who may be happy to try out new tools that could help them crack a case or rescue a victim. The Policy therefore places an emphasis on the requirement to train all officers and civilian employees to recognize possible AI tools, and ask that they be evaluated prior to any use.

Finally, the Policy was developed through extensive consultations with legal, human rights, and technical experts, as well as the general public, which resulted in over 40 written submissions from members of the public, experts, and community organizations. These consultations resulted in many improvements to the Policy. However, there were some suggestions that we did not adopt.

We've heard suggestions that all biometrics, and in some cases, all instances of AI, should be banned from use by the police. In recommending this Policy to the Board, we found these suggestions fail to fairly balance the potential benefits against the potential risks. The Policy places an onus on the Service to prove that the benefits outweigh the risks, and that the risks can be effectively mitigated. The Policy also places a heavy burden of proof, both pre- and post-deployment of AI tools, that ensures that tools will not be adopted willy-nilly, but only where such an effort is truly justified.

We have also heard from stakeholders concerns about the ability of both the TPS and the TPSB to accurately gauge the risks posed by these tools. These stakeholders suggested that the Board should form an expert panel to evaluate such tools and make recommendations to the Board. In our recommendations to the Board we agreed with the need for an expert panel, but suggested that such a panel should be formed at the provincial level, to ensure both cost-effectiveness and consistency across the Province. We are currently in the process of engaging with other Boards in Ontario, and with Ontario's Information and Privacy Commission, to explore options for such a panel.

The TPSB, in approving this Policy, took a crucial first step towards the protection of rights and freedoms of Canadians while enabling the police to effectively protect people and enforce the law. But the Policy was developed without the benefit of an existing legal framework or even best practice models. Lacking these, Canadians will face an inconsistent patchwork of policies over a matter that is critical for their rights and freedoms. I look to you, alongside Provincial governments, to contribute to the legal framework that would enable us to improve on this first step, and thank you for exploring this matter.

Facial Recognition
Parliamentary Appearance – House of Commons Standing Committee on Access to Information, Privacy and Ethics
April 28, 2022

OPENING REMARKS

- Good afternoon Mr. Chair and Honorable members of the Committee, I am grateful for the opportunity to speak with you today on this important issue, which I hope will inform your study into the use and impacts of facial recognition technology.

- As a concept, facial recognition has been used in policing for as long as policing has existed. At its root, facial recognition is the basis of eye witness testimony, police line ups, and "mug" shots, and relies on the ability of a witness to compare various images of people's faces to the person they saw, based on the witness' recollection.

- This technique continues to be employed today to support criminal investigations and the RCMP maintains a national database of lawfully collected criminal record information, including photographs, fingerprints and other biographical information for this purpose.

- With advanced artificial intelligence and machine learning technologies, we are seeing the growth of new biometric analysis tools that allow for a more quantified comparison or matching of images and video, such as Facial Recognition Technology or FRT. The unprecedented increase in the prevalence of digital technology in the daily lives of Canadians also means that there is an increasingly abundant amount of digital imagery available to criminal investigators.

- FRT offers a new and significant opportunity for all law enforcement, particularly in an organization with diverse mandate, such as the RCMP with applications extending from the identification of the victims of child sexual exploitation, to the investigation of violent crime, FRT has the potential to greatly augment existing investigative techniques.

- This said, the RCMP is firmly of the position that this technology must not be used indiscriminately. FRT should only be used in a targeted and time limited fashion for a specific purpose and in a manner consistent with *Charter* and the Canadian privacy protection framework. This technology should not be used to collect personnel information from Canadians without specific cause.

- Despite the fact that FRT has been around for a relatively long time, it should still be considered an emerging technology. Systems developed to-date have been known to suffer from inaccuracies and bias that can result in false positive results. For this reason, the RCMP has never used the results of an FRT match as confirmed identity, instead requiring trained examiners to assess possible matches to determine their veracity.

- Simply put: FRT can produce an investigative lead but trained investigators still need to determine and confirm relevance and accuracy in the course of their investigation, and corroborate an identification through other investigational means.

- While new technology can enhance our ability to conduct investigations more efficiently and effectively, we recognize that our primary obligation is to ensure all policing activities are lawful and conducted in accordance with the *Charter*, *Privacy Act* and all other relevant laws, regulations and policies.

- From October 2019 to July 2020, the RCMP made limited use of a facial recognition technology, Clearview AI, to support our National Child Exploitation Crime Centre, or NCECC, with the identification of victims of online child sexual exploitation.

- I would first like to acknowledge that our initial disclosure of the use of this tool was incomplete. It was not intended to be so.

    - When initially responding to media enquiries and the Privacy Commissioner, it was not commonly known that, across such a large organization as the RCMP, a limited number of programs had begun using Clearview AI, whether with a paid licence or on a trial basis. We responded in error to the Privacy Commissioner and early media enquiries based on an incomplete survey of RCMP program areas.

    - Once we became aware of the broader use of Clearview AI, a more fulsome survey of all RCMP programs and Divisions was made to understand the full extent of the use of Clearview AI within the RCMP. We also immediately notified the Office of the Privacy Commissioner (the OPC).

- The use of Clearview AI by the RCMP was not widespread. The RCMP had a total of twenty (20) licences for Clearview AI – two (2) paid and eighteen (18) trial licences available at no cost only to law enforcement agencies.
    - 65% of the twenty licenses (13) were used for victim identification by the NCECC, seven (7) were trial licences associated with Internet Child Exploitation units in Divisions across the country.

- As you are aware, the OPC conducted an investigation on the RCMP's use of Clearview AI. The RCMP has worked cooperatively with the Privacy Commissioner on this investigation and we welcomed the recommendations of their report.

- The Privacy Commissioner made a number of recommendations for improvements to our current training and operational processes, including the creation of a centralized and standardized process for identifying, tracking, assessing and reporting new technologies that make use of personal information.

- We have fully accepted the recommendations of the Privacy Commissioner and view their implementation as an opportunity to strengthen our existing policies and processes.

- As a key part of our response to the OPC, we have established the National Technology Onboarding Program (or NTOP), to centralize the tracking of new operational tools being used or considered for use across the RCMP. NTOP establishes a standardized process for the implementation of developed or procured technologies and services, including legal, technical and policy assessments, GBA+ and privacy analysis. This is a significant undertaking, but we are hopeful that NTOP will be fully operational this fall. We continue to work closely with the OPC as we implement these recommendations.

- We recognize that technology can and does outpace legislation and regulation. For some existing biometric tools, such as fingerprints and DNA, the government has developed strong legislative and regulatory frameworks that delineate how federal agencies are permitted to use these tools. However, as newer techniques have become available, particularly those involving the use of digital information and media, the legislation has not kept pace, leaving a void that departments and agencies have been left to fill.

- The use of biometric tools that leverage images and videos (such as facial recognition, gait analysis, and voice print analysis) could be significant tools that benefit criminal investigations and, help to bring justice to victims of crime. With NTOP we hope the RCMP can demonstrate its commitment to transparency, accountability and leadership across law enforcement on how to identify and work with our government partners, including the Privacy Commissioner, to implement new solutions.

- Thank you. I am happy to answer any questions you might have.

Published under the authority of the Speaker of
the House of Commons

SPEAKER'S PERMISSION

Also available on the House of Commons website at the
following address: https://www.ourcommons.ca

Publié en conformité de l'autorité
du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Aussi disponible sur le site Web de la Chambre des
communes à l'adresse suivante :
https://www.noscommunes.ca