HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

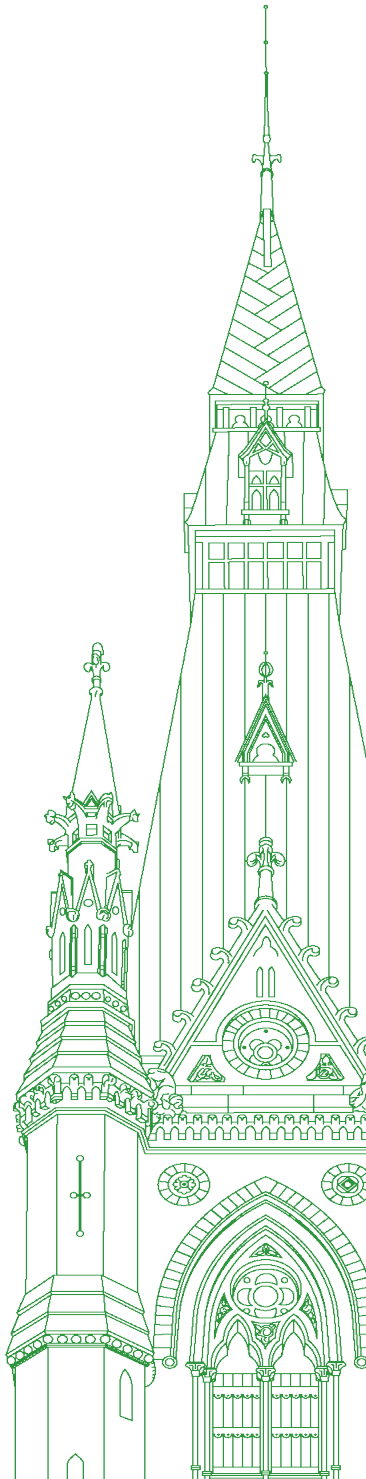
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 018

Monday, May 2, 2022



Chair: Mr. Pat Kelly

Standing Committee on Access to Information, Privacy and Ethics

Monday, May 2, 2022

● (1105)

[*English*]

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

Welcome to meeting number 18 of House of Commons Standing Committee on Access to Information, Privacy and Ethics. Pursuant to Standing Order 108(3)(h) and the motion adopted by the committee on Monday, December 13, 2021, the committee is resuming its study of the use and impact of facial recognition technology.

Today's meeting is taking place in a hybrid format pursuant to the House order of November 25, 2021. The members are attending both in person in the room and remotely by using the Zoom application. Per the directive of the Board of Internal Economy on March 10, 2022, those attending the meeting in person must wear a mask, except for members who are at their place during proceedings.

I would like to make a few comments for the benefit of witnesses and members. First, wait until I recognize you by name before speaking. For those participating by video conference, click on the microphone icon to activate your mike, and please mute yourself when you are not speaking.

For interpretation for those on Zoom, so that you are aware, you have the choice at the bottom of your screen of having just the floor audio, or you can select English or French. For those in the room, use your earpiece and select the desired channel as you normally would.

Now I would like to welcome our witnesses. From the Office of the Privacy Commissioner of Canada, we have Daniel Therrien, Privacy Commissioner of Canada, and David Weinkauf, senior information technology research analyst.

From the office of the Information and Privacy Commissioner of Ontario, we have Patricia Kosseim, commissioner, and Vance Lockton, senior technology and policy adviser.

From the Commission d'accès à l'information du Québec, we have Diane Poitras, president.

Now we'll go to our first witness. Each witness may deliver an opening statement of up to five minutes.

Go ahead, Commissioner Therrien. You have the floor.

[*Translation*]

Mr. Daniel Therrien (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): Good morning, Mr. Chair.

Thank you for inviting me here today and for undertaking this important work on facial recognition.

Like all technologies, FRT can, if used responsibly, offer significant benefits to society. However, it can also be extremely intrusive, enable widespread surveillance, provide biased results and erode human rights, including the right to participate freely, without surveillance, in democratic life. It is different from other technologies in that it relies on biometrics, permanent characteristics that, contrary to a password, cannot be changed. It greatly reduces personal autonomy, including the control individuals should have over their personal information. Its use encompasses the public and the private sectors, sometimes for compelling purposes like the investigation of serious crimes or proving one's identity, sometimes for convenience.

The scope of your study is vast. In the time I have available, I will focus on the use of FRT in a law enforcement context. When we last spoke, my office had completed its investigation into Clearview AI, a private sector platform that we and our colleagues in Quebec, B.C. and Alberta found was involved in mass surveillance.

Since then, my office has examined the RCMP's use of Clearview AI's technology. We found that the RCMP did not take measures to verify the legality of Clearview AI's collection of personal information, and lacked any system to ensure that new technologies were deployed lawfully. Ultimately, we determined the RCMP's use of Clearview AI to be unlawful, since it relied on the illegal collection and use of facial images by its business partner.

[*English*]

Building on these findings, we worked with fellow privacy commissioners across Canada to develop joint guidance for police use of facial recognition. This guidance is meant to assist police in ensuring that any use of the technology complies with the law, minimizes risks and respects privacy rights. We are releasing the final version of the guidance today.

As part of this work, we launched a national public consultation on police use of facial recognition technology. During this consultation, we heard consistently that the current laws regulating the use of facial recognition did not offer sufficient protection against the risks associated with the technology. While all stakeholders we consulted agreed that the law must be clarified, there was no consensus on the content of a new law. Legislators will therefore have to decide how to reconcile various interests.

Following this consultation, fellow provincial and territorial privacy commissioners and I believe that the preferred approach should be to adopt a legislative framework based on four key elements, which we have outlined in a joint statement we're issuing today.

First, we recommend that the law clearly and explicitly define the purposes for which police would be authorized to use facial recognition technology and that it prohibit other uses. Authorized purposes should be compelling and proportionate to the very high risks of the technology.

Second, since it is not realistic for the law to anticipate all circumstances, it is important, in addition to limitations on authorized purposes, that the law also require police use of facial recognition to be both necessary and proportionate for any given deployment of the technology.

Third, we recommend that police use of facial recognition should be subject to strong, independent oversight. Oversight should include proactive engagement measures such as privacy impact assessments, or PIAs; program level authorization or advance notification before use; and powers to audit and make orders.

Finally, we recommend that appropriate privacy protections be put in place to mitigate risks to individuals, including measures addressing accuracy, retention and transparency in facial recognition initiatives.

I encourage you to consider our recommendations as you complete your study of this important issue.

● (1110)

[*Translation*]

Thank you for the opportunity to appear before you today; I look forward to your questions.

I will be pleased to answer your questions following my colleagues' statements.

[*English*]

The Chair: Thank you.

Now, for up to five minutes, we have Commissioner Kosseim.

[*Translation*]

Ms. Patricia Kosseim (Commissioner, Office of the Information and Privacy Commissioner of Ontario): Good morning.

Thank you for inviting me to speak today.

Joining me is Vance Lockton, senior policy and technology analyst with my office.

I would like to build on the remarks you've just heard from Commissioner Therrien. While all of Canada's Privacy Commissioners recommend the adoption of a comprehensive statutory framework to address the use of facial recognition technology in the criminal law context, we also recognize that some police agencies are already using, or considering using, facial recognition technologies. As such, we have issued guidelines to help guide law enforcement agencies and mitigate against potential harms until a new statutory framework is put in place, as my colleague Mr. Therrien described it.

I would like to emphasize five key elements of the guidelines.

First, before using facial recognition for any purpose, police agencies must establish that they are lawfully authorized to do so. This is not a given, and cannot be assumed. Facial recognition relies on the use of sensitive biometric information. Police should seek legal advice to confirm they have lawful authority either at common law or under statutes specific to their jurisdiction. They must also ensure they are Charter-compliant and their purported use is necessary and proportionate in the circumstances of a given case.

[*English*]

Second, police agencies must establish strong accountability measures. This includes designing for privacy at every stage of a facial recognition initiative and conducting a privacy impact assessment, or PIA, to assess and mitigate risks in advance of implementation.

It also involves putting in place a robust privacy management program, with clearly documented policies and procedures for limiting the purposes of facial recognition, robust systems for logging all related uses and disclosures, and clearly designated roles and responsibilities for monitoring and overseeing compliance.

Such a program must be annually reviewed for its continued effectiveness. It must be supported by appropriate training and education, and ensure that any third party service providers also comply with all related privacy obligations.

Third, police agencies must ensure the quality and accuracy of personal information used as part of a facial recognition system to avoid false positives, reduce potential bias and prevent harms to individuals and groups. Ensuring accuracy involves conducting internal and external testing of the FR system for any potentially discriminatory impacts, as well as building in human review to mitigate risks associated with automated decisions that may have a significant impact on individuals.

Fourth, police agencies should not retain personal information for longer than necessary. This means destroying probe images that don't register a match and removing face prints from the database as soon as they no longer meet the proper criteria for inclusion.

Fifth, policy agencies must address transparency and public engagement. Direct notice about the use of facial recognition may not always be possible in the context of a specific police investigation. However, transparency at the program level is certainly possible, and could include publishing the agency's formal policies on the use of facial recognition, a plain language explanation of their program and a summary of their PIA,.

Any communication with the public should be two-way. Key stakeholders, particularly representatives of over-policed groups, should be consulted in the very design of the facial recognition program. Given the special importance of reconciliation in Canada, this must include input from local indigenous groups and communities.

These are a few of the measures set out in the guidance.

To reiterate, although we believe these guidelines represent important risk mitigation measures, ultimately we recommend the establishment of a comprehensive statutory regime governing the use of facial recognition by police in Canada. Clear guardrails with force of law are necessary to ensure that police agencies can confidently make appropriate use of this technology, grounded in a transparent framework, accountable to the people they serve and capable of earning the public's enduring trust.

Thank you.

[*Translation*]

The Chair: Thank you.

The president of the Commission d'accès à l'information du Québec, Ms. Diane Poitras, now has the floor for five minutes.

● (1115)

Mrs. Diane Poitras (President, Commission d'accès à l'information du Québec): Thank you, Mr. Chair.

Good morning and thank you for this invitation to discuss facial recognition.

Building on my colleagues' remarks, I would briefly like to address the problems raised by other uses of this technology and to outline what is provided under Quebec legislation. As several speakers have mentioned, the increasingly widespread use of facial recognition in various contexts raises significant problems, particularly with respect to privacy.

This technology, which combines biometrics with artificial intelligence, among other things, is particularly invasive, partly because it scans unique body characteristics and transforms them into data. Those characteristics, such as certain facial traits, are central to our identity. The fact that this technology can be used without our knowledge means we have less control over our information and are at greater risk of undue surveillance. Some proposed uses of facial recognition and derivative technologies infer from our face or facial expressions personal characteristics such as age, sex, ethnic origin, emotions, degree of attention, fatigue or stress, health information and certain personality traits. These characteristics may be used to categorize, detect or profile individuals for commercial purposes to conduct some form of surveillance or to make decisions concerning them.

The creation of biometric databases also raises significant privacy risks. It is difficult for a person whose biometric data have been compromised to challenge an inadvertent action or transaction or identity fraud given the high degree of reliability that unique and permanent information is assumed to have. Since it is virtually impossible to replace compromised biometrics, it can be just as complicated to re-establish one's identity.

There is also considerable risk that biometric databases created for one specific purpose may be used for other purposes without our knowledge or an adequate assessment of the problems and risks associated with those other purposes. This is why the creation of these banks and the use of biometrics for identification purposes are governed in Quebec by the Act to establish a legal framework for information technology, as well as privacy statutes applicable to public and private organizations. The creation of every biometric database must thus be reported to the commission. Starting next September, reporting will also be required for every instance in which biometrics are used for identification purposes.

In Quebec, biometrics may not be used for identification purposes without the express consent of the person concerned. No biometric characteristic may be recorded without that person's knowledge. Only a minimum number of biometric characteristics may be recorded and used. Any other information that may be discovered based on those characteristics may not be used or preserved. Lastly, biometric information and any note concerning that information must be destroyed when the purpose of the verification or confirmation of identity has been achieved. The commission has broad authority and may make any order respecting biometric banks, including authority to suspend or prohibit their bringing into service or order their destruction. General privacy protection rules also apply in addition to these specific provisions. That means, for example, that the use of facial recognition must be necessary and proportionate to the objective pursued.

We have observed that organizations unfortunately do not attach all the importance they should to this compliance evaluation or the problems associated with the use of facial recognition. The popularity of biometrics has led to a kind of trivialization of its impact on citizens, which is why the commission recommends that a preliminary analysis be conducted of privacy-related factors. That evaluation will in fact be mandatory as of September 2023. Biometric information will also be expressly designated as sensitive personal information. Although the current regulation of biometrics in Quebec has given the commission an idea of the extent of facial recognition use and grants it enforcement powers, we have requested that regulation be enhanced to reflect developments in the technology and the various contexts in which it is used.

Thank you for your attention. I will be pleased to discuss these matters with you over the next few minutes.

● (1120)

[*English*]

The Chair: With that, we'll go straight to questions.

Mr. Kurek, you have up to six minutes.

Mr. Damien Kurek (Battle River—Crowfoot, CPC): Thank you very much.

I appreciate the presence of all of the commissioners today, and their expertise.

To all the witnesses, I'm hoping we would be able to get a copy of that joint statement to enter it into testimony. Could you just confirm that it can be done? Thank you very much.

Commissioner Therrien, over the last number of meetings in this study, we've learned and heard a lot about some of the challenges associated with facial recognition technology. You've referenced the consultations that were done. Could you outline for the committee what that consultation looked like in terms of facial recognition technology and its use, some of the stakeholders who were involved in that consultation and some of the trends that you might have noticed during that process?

Mr. Daniel Therrien: Sure.

When we issued our investigative report on the RCMP's use of Clearview last June in a special report to Parliament, we started at the same time a consultation with stakeholders who were interested in speaking to draft guidance that we had published at the same time. That led to about 30 groups or individuals writing to us, and we also had meetings with a number of stakeholders.

The stakeholders represented civil society, minority groups and the police itself. I met a number of times with the RCMP and with the Canadian Association of Chiefs of Police, and my colleagues also met with provincial equivalents. There was a broad range of people who were consulted. Views were varied, obviously, because the interests were different, but all agreed that the law is insufficient as it is. Depending on the interests of various stakeholders, they did not agree necessarily on the content of that law.

Mr. Damien Kurek: Sure, and in your opening statement you said that there was no clear consensus found by stakeholders, and certainly that's the sentiment that I've found as we've heard from different witnesses. We did hear the RCMP very clearly say that they had disagreed with your office's findings in terms of their use of Clearview AI.

I'm curious if you could share with the committee some of your observations about the trends that you found when consulting with the wide variety of groups that you've engaged with in this process.

Mr. Daniel Therrien: I would start first with where there was agreement beyond the need for the law to be changed.

Many people felt that the guidance was drafted or crafted at a level of generality such that the advice is helpful, but they would like it at the very least to be supplemented by advice on what was called “use cases”. Our reaction to that is that indeed there is a need for advice on particular uses in different contexts, because context matters a whole lot, but we still think it's important and relevant to have general guidance that can be be augmented as use cases are developed.

Some stakeholders from civil society or minority groups called for a moratorium on the use of facial recognition. The RCMP obviously did not agree with that. Our position as commissioners is that there should be clear laws prescribing when facial recognition can be used, because it can be used for legitimate, helpful purposes and social good in some circumstances—for instance, in serious crime situations or to find missing children—but these uses should be defined quite narrowly. The law should also prescribe prohibited uses, which would be, I guess, a partial ban or a partial moratorium on the use of facial recognition.

If I may, on the question of a moratorium, we as data protection authorities cannot impose a moratorium that has the force of law. For a moratorium to be binding on police agencies, it would have to take the form of legislation.

I was struck by the testimony that you heard last week from an RCMP representative, to the effect that “The RCMP believes that the use of facial recognition must be targeted, time-limited and subject to verification by trained experts.”

● (1125)

Mr. Damien Kurek: I'll ask one question now because of time limitations. Would you be able to provide the committee with a list of best practices from other jurisdictions around the world that already have some of these frameworks, for the committee to be able to reference and point to?

Mr. Daniel Therrien: Sure.

Mr. Damien Kurek: I apologize; I think I'm basically out of time.

Thank you very much to all of the witnesses for coming today and for your expertise. Thank you.

The Chair: Mr. Fergus, go ahead for six minutes.

[*Translation*]

Hon. Greg Fergus (Hull—Aylmer, Lib.): Thank you very much, Mr. Chair.

Thanks as well to Mr. Therrien, Ms. Kosseim and Ms. Poitras for their testimony today.

I will go first to Mr. Therrien, then to the other two witnesses.

Mr. Therrien, I know you've submitted a report on the use of facial recognition by the RCMP, and I thank you for that. I found it very interesting and useful. However, I'd like to take a step back so I can apply that to everyone, both governments and the private sector, as Quebec's legislation attempts to do.

Do you think the advice you gave the RCMP on the use of facial recognition would generally apply to the private sector?

Mr. Daniel Therrien: I think the common factor that applies horizontally to all stakeholders who would like to use facial recognition is the principle of necessity and proportionality that my two colleagues mentioned. That applies to all stakeholders: police services, businesses and other departments and governments.

In police services, however, the use of facial recognition can have extremely serious consequences, resulting even in the loss of freedom. I would say that many common principles should be considered. All stakeholders, including legislators, had to consider the context and consequences of the use of this technology. For example, a total prohibition of its use by police services in certain circumstances might not necessarily apply to all stakeholders.

Hon. Greg Fergus: I agree with you that the use of facial recognition by police services may raise serious issues.

We heard from witnesses from Princeton University in the United States who said that, while governments play a leading role in the use of this technology, private businesses also have a role. For example, there can be serious consequences if you use it to determine what kind of credit risk a citizen presents. Its use is based on a theory that's built on evidence that's insufficient to justify that use.

Ms. Kosseim, thank you very much for citing the five key elements in the guidelines. Do you think they may also apply to the private sector?

Ms. Patricia Kosseim: Thank you for your question.

As my colleague said, the principles should definitely apply, regardless of the sector concerned, obviously considering the context and range of risks at play. I would note that Ontario doesn't have a privacy act that applies to the private sector. However, my office very much agrees with the idea the government has proposed of one day passing one.

In privacy matters, most businesses are subject to federal legislation. However, that leaves a vacuum in many areas in Ontario. In many sectors, there is no legislation protecting the privacy of employees in the vast majority of businesses. So that's a major deficiency. I think it's important that the basic principles we advance in our guidelines apply and that we proceed with the necessary adjustments for other contexts. Our guidelines are specifically designed for the law enforcement sector and police services.

● (1130)

Hon. Greg Fergus: Thank you.

Ms. Poitras, I applaud your bill, which would require businesses to comply with the directives provided under the act by 2023.

I know I'm putting you in an uncomfortable position by asking you this question, but can we do more in Quebec or in the federal government to protect citizens from the issues associated with facial recognition technology?

Should the federal government pass legislation similar to what you have in Quebec?

Mrs. Diane Poitras: Thank you for your question.

The Quebec act is definitely a start, but we've previously submitted recommendations for improving it to Quebec parliamentarians. For example, the framework currently establishes obligations only where biometrics and facial recognition are used to verify identity. However, based on the reports we receive from biometric databases, the technology is also being used for other purposes. I mentioned that in my presentation. Consequently, the first recommendation would be to ensure—

The Chair: I'm sorry.

Hon. Greg Fergus: Mr. Chair, would you please ask the witnesses to forward in writing any further information they may have for the committee?

The Chair: All right.

[*English*]

Mr. Fergus, you did not permit very much time for this witness to answer that question. I'm sorry, but we will have to move on.

[*Translation*]

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

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

Thanks to all the commissioners for being here today.

I congratulate them for publishing the guidelines, a document that we've been waiting for.

Mr. Therrien, in a few words, how would you define what surveillance is?

Mr. Daniel Therrien: When surveillance is carried out by police services or private companies, they collect information about people's activities or characteristics in order to make certain decisions about them.

The question is whether it's done with people's consent or in accordance with legislation that protects the rights of citizens who are exercising these rights. That, in my opinion, is the key. Consumers, vis-à-vis companies, and citizens vis-à-vis the state, should be able to exercise their right to use social media, communicate and take part in demonstrations, without being subjected to mass surveillance, except in extremely limited circumstances.

Mr. René Villemure: Thank you very much.

Similarly, we were told, in connection with police officers who were recording what demonstrators were doing, that it was for the archives. It is nevertheless a form of surveillance.

Mr. Daniel Therrien: Yes.

● (1135)

Mr. René Villemure: Okay.

You were just getting going earlier when you were talking about the RCMP. Having heard testimony from the people who appeared last week, I'd like you to return to that subject.

Mr. Daniel Therrien: On a number of occasions, you were told about a moratorium, whether desirable or otherwise, that was going to be applied until an enhanced act was adopted. It's clear to me that a moratorium applicable to police services should be provided for in a law. However, I found it interesting last week when the RCMP representative raised a number of principles governing the use of facial recognition by the RCMP. That's in the English version I'm looking at.

[*English*]

He said it should be “targeted, time-limited and subject to verification by trained experts. Further, [it] should not be used to confirm an identity, but rather only be considered as an investigational aid”.

[*Translation*]

The matter of verification by someone was raised.

You could ask the RCMP to commit to using facial recognition only in accordance with the principles stated by its representative last week. I feel that would be the best way of handling a moratorium while awaiting the enhanced act.

Mr. René Villemure: The principles were nevertheless legitimate.

Mr. Daniel Therrien: Yes.

Mr. René Villemure: Okay.

Thank you, Mr. Therrien.

Ms. Poitras, could you briefly summarize the Clearview AI situation for us, given that it was very important in connection with your work in Quebec?

Mrs. Diane Poitras: Thank you for your question.

As you know, Quebec's access to information commission was involved in the joint investigation, with its counterparts from the federal government, Alberta and British Columbia. After that, we issued an order under our own provincial authority. Our decision was appealed, which is possible in Quebec, and it is currently before the courts.

We would be happy to send you our decision, which explains our position and is up on our website. Unfortunately, as the matter is before the courts, I will refrain from making any comments out of respect for the judicial process.

Mr. René Villemure: Thank you. We would appreciate your sending it.

I won't ask you to reveal any secret information, but can you tell us what Clearview AI is challenging?

Mrs. Diane Poitras: To summarize the decision as a whole, there is the commission's authority to issue the order, since it's an American firm, and also all our legal conclusions pertaining to compliance with Quebec's act.

Mr. René Villemure: Thank you very much.

Mr. Therrien, according to you, is the RCMP already carrying out surveillance.

Mr. Daniel Therrien: I'm going to return to what I heard last week. The RCMP says that it is not doing mass surveillance. I have no reason to doubt this. The RCMP could demonstrate that it is using facial recognition for compelling reasons by committing to using it only for such purposes. I noted last week that the RCMP representative wasn't particularly clear as to whether or not the RCMP is using facial recognition.

At best, I would say that I have no reason to believe the RCMP is using facial recognition for mass surveillance. On the other hand, their definition of the circumstances under which they use it seems rather ambiguous. That, moreover, is why we are sending the guidance document and are recommending that police forces be subject to a clear act that authorizes facial recognition, but also prohibits its use in certain circumstances.

Mr. René Villemure: Thank you very much.

The Chair: Thank you, Mr. Villemure.

[*English*]

Ms. Gazan, welcome to the ethics committee. You have up to six minutes.

Ms. Leah Gazan (Winnipeg Centre, NDP): Thank you so much, Chair.

Monsieur Therrien, your office [*Technical difficulty—Editor*]

● (1140)

The Chair: Your microphone was not activated.

Ms. Leah Gazan: Oh, it was not? I'm sorry.

The Chair: I'm going to reset your time. Go ahead, Ms. Gazan. I'll ask you to restate your question.

Ms. Leah Gazan: Thank you, Chair. Just so you know, this isn't my first committee. I'm sorry, everybody.

Monsieur Therrien, the Office of the Privacy Commissioner published a report in June 2021 entitled “Police use of Facial Recognition Technology in Canada and the way forward”. The report provides a series of recommendations that the RCMP agreed to implement no later than 12 months after receipt of that particular report. Some of the recommendations included a training program to ensure decision-makers are trained on the limitations on collection of personal information under the Privacy Act, policies to clarify who can make decisions on the collection of personal information, and systems to monitor for unauthorized collections.

Could you elaborate on the recommendations you made that the RCMP agreed to and how these will improve privacy practices?

Mr. Daniel Therrien: Thank you for that.

While the RCMP disagreed with our conclusion at law that the RCMP itself was breaching the public sector law by relying on Clearview, they did co-operate significantly with us in recognizing that they should have a better verification system when they use new technologies, be it facial recognition or other new technologies.

We have, I think, agreement with the RCMP that they ought to have these verification systems, and we have had good discussions with them since June of last year. I do not think they will be able to implement all of these recommendations within a year, but we're making good progress.

Ms. Leah Gazan: However, they had agreed to implement them no later than 12 months after receipt of the report. What you're saying is that they have not implemented the recommendations and it has been over 12 months. Am I correct?

Mr. Daniel Therrien: They have not yet, and they are unlikely to meet the 12-month deadline, but we are making good progress, and I see a genuine effort on their part.

It is a relatively complex issue, but we obviously would like to see this implemented as soon as possible.

Ms. Leah Gazan: I'll move on.

In June 2021, the OPC report also stated that:

> There were serious and systemic failings by the RCMP to ensure compliance with the Act before it collected information from Clearview and, more broadly, before novel collection of personal information in general. This includes widespread failures to know what it was collecting, control how collection occurs, identify potential compliance issues, and assess and prevent contraventions of the Act.

The use of the words “systemic” and “widespread” suggests that this isn't a one-off error or a poor decision, so how can we be assured that the RCMP is compliant with privacy laws going forward and that there aren't other cases like Clearview quietly flying under the radar?

I ask that question because the report uses the words “systemic” and “widespread”.

Mr. Daniel Therrien: This language refers back to the absence, at that time, of any system at the RCMP to ensure that when new technology is used by its officers, there is a verification and approval process within the RCMP to ensure that the technology respects the law, including privacy rights.

This was far from ideal, to say the least, but the RCMP has recognized the problem and is setting up such a system. It will take a bit more time than we had hoped, but I think it's going in the right direction.

● (1145)

Ms. Leah Gazan: I find that concerning, because we're dealing with privacy issues. You say that it'll take a bit more time. Could you give us an approximate amount of time?

I ask that because initially they said that they were supposed to put the recommendations in place 12 months after the report. They have not done that. We know that it's systemic and widespread. What duration of time do you think it will take?

Mr. Daniel Therrien: The RCMP has set up a system. It's the implementation of the details of the system—for instance, the training to be given to officers—that is taking more time to define than we had hoped.

I would suggest that you ask the RCMP how long it's going to take. We have asked them ourselves, obviously. I can report on what the RCMP has told us. I can undertake to do that, so I will do that.

Ms. Leah Gazan: Thank you so much. Would you be able to submit that to the committee? Is it possible?

Mr. Daniel Therrien: Yes.

Ms. Leah Gazan: Okay. Thank you so much.

I'm not sure how much time I have, Chair.

The Chair: You have 20 seconds. You have time for a very quick question.

Ms. Leah Gazan: Okay, so I have time.

The Chair: You have to be very quick, though.

Ms. Leah Gazan: In a joint investigation of Clearview....

I don't know how much time I have now.

A voice: None.

Ms. Leah Gazan: None. Okay. Great. Very good. Thank you—

The Chair: We have time today. I'm being a little generous, so go ahead with your question. After a brief question and a brief answer, we'll move on.

Ms. Leah Gazan: Thank you so much, Chair.

In the joint investigation of Clearview by the Privacy Commissioner of Canada, the Information and Privacy Commissioner for British Columbia and the Information and Privacy Commissioner of Alberta, the offices recommended the following: One, cease offering the facial recognition services that have been the subject of this investigation to clients in Canada; two, cease the collection, use and disclosure of images and biometric facial arrays collected from individuals in Canada; and three, delete images and biometric facial arrays collected from individuals in Canada in its possession.

Has Clearview taken any of these actions?

Mr. Daniel Therrien: Clearview stopped offering its services in Canada in 2020, I believe, while we were still investigating, but it is in court challenging the decisions of my colleagues, I believe because they do not want to give an undertaking in perpetuity that they will not offer their services. At this point, they are not offering their services in Canada.

Ms. Leah Gazan: Thank you.

The Chair: Mr. Williams, you have five minutes.

Mr. Ryan Williams (Bay of Quinte, CPC): Thank you, Mr. Chair, and through you to Mr. Therrien as well.

As you mentioned, last week we had the RCMP before us. In response to the findings that the RCMP's use of Clearview AI was illegal, they said they disagreed with your findings. A representative reiterated that stance.

Does the reason for disagreeing with your findings have any merit, and why or why not?

Mr. Daniel Therrien: I'll give a lawyerly answer, which I think will be clear.

The provision at play is the provision of the Privacy Act that governs the collection of information, in this case by the RCMP. What the RCMP is saying is that this section, section 4 of the Privacy Act, does not explicitly require a federal institution such as the RCMP to ensure the legality of the practices of its commercial partner before the public sector uses the information.

It is true that section 4 does not explicitly require that of a federal institution; we think that the requirement exists implicitly. Essentially, imagine that federal institutions would be able to contract out and be able, through contracting with the private sector, to engage in practices that it cannot engage in directly. That is unacceptable. We think the law does not allow for that.

That said, is it credible or is it reasonable? There is some credible basis for the RCMP's position. To the extent that there is ambiguity in the law, I would encourage you strongly to close that loophole and to require government institutions—not only the RCMP, but all government institutions—to ensure that what they're buying is lawful when they rely on the private sector.

● (1150)

Mr. Ryan Williams: Thank you.

As a follow-up question, should the powers of your office be strengthened so that the rulings on Privacy Act violations are binding and properly enforced, since they seem to have ignored them?

Mr. Daniel Therrien: The short answer is yes. We've recommended that many times. Yes.

Mr. Ryan Williams: Okay.

With regard to just a little bit more data on its use by the RCMP, are you aware of how many convictions they made using evidence collected by Clearview AI?

Mr. Daniel Therrien: No, I am not. We asked how many times they'd used it, and I believe it was in the tens of cases. As to the convictions, no, I do not know the number.

Mr. Ryan Williams: In your opinion, just knowing how they collected it, could their collection and use of Clearview AI's facial recognition technology risk overturning convictions of any criminal caught or prosecuted using data collected by Clearview?

Mr. Daniel Therrien: I think that's speculative. The RCMP says, which I have no reason to doubt, that when they use the technology, there's human review. That tells me that there's a police officer who then undertakes an investigation and presents evidence through a Crown attorney under the normal rules. That's my assumption, but I don't know that.

Mr. Ryan Williams: The RCMP told this committee last Thursday that Clearview AI was the only modern FRT system they were using, but when asked could not detail other non-modern FRT systems. Through your investigation, are you aware of other FRT systems that the RCMP is using?

Mr. Daniel Therrien: We're not aware of other FRT systems that the RCMP is using. There are, of course, many FRT systems other than Clearview, but they do not all have the same level of accuracy, which is a concern.

As far as the RCMP is concerned, we do not know that they are using a system other than Clearview. They are not currently using Clearview.

Mr. Ryan Williams: Thank you.

Ms. Kosseim, do we know how Ontarians' images are being gathered and stored at this point? Companies using FRT are gathering images. Do we know how they're gathered and stored in Ontario?

Ms. Patricia Kosseim: Unfortunately, I don't have insight into companies in Ontario, because that's not in our jurisdiction. I can't answer that question with any certainty.

Mr. Ryan Williams: I'll stick to the public sector, then. Do we know how they're being stored?

Ms. Patricia Kosseim: Is that in general or in using facial recognition technology?

Mr. Ryan Williams: I think in general, including FRT.

Ms. Patricia Kosseim: I'll give you a couple of examples.

Certainly police services are using images in mug shot databases pursuant to their powers under the Identification of Criminals Act. There is also obviously much video surveillance that is ongoing in terms of general, municipal and other collection of video surveillance. That too is fairly common and ongoing in terms of collection of video surveillance and therefore images of people.

Mr. Ryan Williams: Thank you very much.

Thank you, sir.

The Chair: Thank you.

Ms. Hepfner, you have five minutes.

Ms. Lisa Hepfner (Hamilton Mountain, Lib.): Thank you very much.

[*Translation*]

I'd like to thank all the witnesses here with us today.

I'll begin with Mr. Therrien, but will do so in English because it's easier for me.

[*English*]

You talked about how all the stakeholders you consulted with agreed that privacy legislation in Canada needs to be updated. It makes sense, because when it was drafted, we didn't know about facial recognition technology.

I'm wondering what sort of advice you have for legislators to be flexible in the legislation so that we don't have to rewrite the legislation every time a new piece of technology comes. How do we make it flexible so that when there are more advancements in technology, the legislation still applies?

Mr. Daniel Therrien: That's a good question.

My starting point would be to say that we do have laws. Obviously, we have the charter and we have the common law, and there are some statutes like the RCMP Act that govern the situation. In the private sector, we have PIPEDA.

To your point about flexibility to ensure that the law does not become obsolete, one of the virtues of PIPEDA is that it is principles-based, so it does not seek to regulate particular situations but deals with principles. However, I think facial recognition is where we start to see the limits of the virtues of a principles-based approach, because if you regulate facial recognition by saying that the user ought to be accountable, or you apply principles of that nature or say that a necessary proportionality should apply, you leave a lot of discretion to the police to exercise these broad principles in a way that suits their interests.

I'm not saying there ought not to be principles-based legislation. As a general principle, it makes a lot of sense, but in the case of facial recognition, because of the extremely high risks to privacy and other rights, such as democratic rights of demonstrating or equality rights, we say that there ought to be specific provisions—for instance, in the case of the police—to prohibit uses except in certain circumstances.

A good grounding of principles-based legislation makes sense, but in the case of facial recognition it should include the addition of a few specific rules that ensure that the broad principles are not abused or not interpreted in an overly generous way.

● (1155)

Ms. Lisa Hepfner: Very good. That's helpful. Thank you.

I know that the Competition Bureau is also looking at the changes in privacy issues brought on by technology. Can you talk to us about whether you have a relationship with the Competition Bureau and if your office is working in conjunction with that office to tackle some of these issues?

Mr. Daniel Therrien: The short answer is yes, we do work with the Competition Bureau. We have discussions with them fairly regularly, but both of us, the bureau and the OPC, are limited by our current laws in that we are not able to share, for instance, detailed information that we gather in the context of an investigation because we're both bound by a confidentiality rule that prevents us from sharing with the other regulator the details of what we affirm.

We can have discussions at a level of general principle. We can talk about general trends, but it would be extremely helpful, as both of us have recommended in previous months and years, to be able to share what we have learned through investigations so that our collaboration could be more effective.

Ms. Lisa Hepfner: I have 30 seconds left, so I'll go quickly.

You said you were moved by the RCMP's saying that FRT should be targeted, time-limited and subject to verification by trained experts. In what ways is FRT used for good, as in your examples of fighting crime or finding missing children? In what ways is this technology used in an acceptable way?

Mr. Daniel Therrien: As far as the police are concerned, I think those two examples would be the most important ones. As for “crime”, I would qualify that and say “serious crime”. I'm not sure that facial recognition should be used for common theft, for instance, given the risks of the use of facial recognition for privacy and other democratic rights, but it can certainly be acceptable for serious crimes, such as missing children, and for other compelling state purposes, such as in the border context to ensure that people of concern can be identified at the border while not impeding the flow of travellers to the country. To me, the necessity of identifying people of concern at the border in that context would be a compelling ground.

The Chair: Thank you, Commissioner. That was another round with generous time, but I think we have the ability to do that today.

Go ahead for your round of two and half minutes, René.

● (1200)

[*Translation*]

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

Mr. Therrien, I'm going to be brief, but if you could send us information afterwards, that would be great.

We talked about Clearview AI, which left the country for someplace where it would not be subject to our legislation, but there are also companies like Palantir, which are major players in the facial recognition and data management industry.

Are these companies able to self-regulate?

Mr. Daniel Therrien: No.

Mr. René Villemure: Ethics is not a concern for these companies, which are relatively open about their willingness to use data in an unlimited way, I believe.

Mr. Daniel Therrien: In fact, I think that's one of the lessons we can learn from how the technology has been used in recent years. We have to put a stop to self-regulation by companies, and those in the surveillance field deserve particular attention. Generally speaking, elected representatives need to regulate the use of the technology. That's the main lesson to be drawn from the past few years.

Mr. René Villemure: Can you tell us a bit about Palantir, which is still a Government of Canada supplier?

Mr. Daniel Therrien: It's clear that we are greatly concerned about Palantir's practices, but as we haven't investigated the company, I don't feel comfortable commenting about it.

Mr. René Villemure: Ms. Kosseim, have you investigated Palantir?

Ms. Patricia Kosseim: No.

Mr. René Villemure: How about you, Ms. Poitras?

Mrs. Diane Poitras: No.

Mr. René Villemure: Okay.

In connection with the four elements you mentioned earlier, you said that there was an entity responsible for oversight.

What entity are you referring to?

Mr. Daniel Therrien: As the authorities on protecting information, we believe that we will have a role to play in protecting personal data. However, facial recognition brings other rights into play, such as the right to equality in cases of discrimination against certain groups, and also democratic rights.

So we are not asking for a monopoly on facial recognition regulation, but I think that, as in other areas, it would be both possible and useful to have a number of regulatory organizations. In cases of discrimination, for example, it would be the Canadian Human Rights Commission or its provincial counterparts.

So we think we have a role to play in data protection, but other regulatory agencies should also have responsibilities.

Mr. René Villemure: So there ought to be a set of organizations that could together constitute another entity.

[*English*]

The Chair: Thank you.

We go now to Mr. Green. It's nice to have you back. Go ahead for two and a half minutes.

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

Mr. Chair, we've heard in a previous answer by a witness today that a private industry is not able to regulate itself. You'll recall that in previous testimony, the RCMP disagreed with the findings of the Privacy Commissioner about violations that were present, so I want to ask the Office of the Privacy Commissioner about this.

The OPC found that the RCMP's use of Clearview AI contravened the Privacy Act and PIPEDA. The RCMP testified that they disagreed with the findings of the investigation. Through you, Mr. Chair, why does the OPC believe that the RCMP violated the Privacy Act and PIPEDA?

Mr. Daniel Therrien: The RCMP is saying that the Privacy Act does not explicitly require it to verify the legality of the practices of its private sector contractors. It is true that the Privacy Act does not explicitly say that. We are of the view that a correct interpretation of that law is that they do have that responsibility, and if there is any ambiguity in the law, I would strongly urge parliamentarians to close that loophole and make it clear, as I suggested a few minutes ago.

Mr. Matthew Green: In other words, they can't do indirectly what they can't do directly. Is that correct?

● (1205)

Mr. Daniel Therrien: Exactly.

Mr. Matthew Green: Yet here we are, with a scenario in which we know that police services are using this surreptitiously through many ways of procurement, through purchases and also through trial examples as well.

We heard the RCMP state in their testimony that they had no idea who signed off on the use of this technology. Are you aware of any other police agencies in Ontario that currently use Clearview?

Mr. Daniel Therrien: Clearview has stated to us that they have left the Canadian market. They are not offering their services at this point to anyone in Canada.

Mr. Matthew Green: How would you close the loop specifically to ensure that these breaches of privacy, information and civil liberties aren't breached again in the future, not just by the private sector but most clearly through our law enforcement?

Mr. Daniel Therrien: Today I, along with provincial and territorial commissioners, have made a number of recommendations to amend the law. I think it should be done urgently, because the risks are very important.

It starts with better laws. Until such time as laws are amended, we have issued guidance on how to use the current law, and we hope this guidance will mitigate risk.

Mr. Matthew Green: Thank you so much.

The Chair: Thank you.

Now we go to Mr. Bezan for five minutes.

Mr. James Bezan (Selkirk—Interlake—Eastman, CPC): Thank you, Mr. Chair.

I want to thank our witnesses for their presentations and their participation in this important study. The announcement you made jointly earlier today definitely couldn't have been timed better, considering the work we're doing right now.

Mr. Therrien, to follow up on Mr. Green's questioning, you said the RCMP was unlawfully using Clearview technology. Were any penalties assigned to the RCMP—or to Clearview, for that matter?

Mr. Daniel Therrien: No, but we should look at this as an institutional issue. I would tend to look at it through the eyes of the institution, rather than in terms of individuals.

We've made recommendations for the RCMP to improve its processes, but I'm not aware of any sanctions.

Mr. James Bezan: Are you aware of the organization IntelCenter and the IntelCenter database of facial recognition technology?

Mr. Daniel Therrien: Personally, I am not. Perhaps some of my colleagues at the OPC are aware of it. We can provide information if we have any.

Mr. James Bezan: Based upon access to information requests that we just got back, it appears that the RCMP, CSIS and the Department of National Defence are making use of this technology. I think it's something we need to dive into as well.

Their own documents suggest that they use open-source images to identify things like terrorists from the Internet and then provide that to law enforcement agencies like the RCMP and CSIS.

Mr. Daniel Therrien: If we have information, we'll provide it.

Mr. James Bezan: You can maybe take that under advisement.

When you talk about amending existing legislation, you're talking about the Privacy Act and PIPEDA. Should it be extended to include the Criminal Code?

Mr. Daniel Therrien: Possibly. I haven't thought about the exact pieces of legislation that need to be amended.

As I responded in answering an earlier question from Ms. Hepfner, I think we need to start from a principles base, augmented with a few provisions to ensure that general principles cannot lead to overly generous interpretation. It means definitely PIPEDA and the Privacy Act, and potentially the Criminal Code.

There is a lot of authority in the common law for the use of various technologies. Potentially, the Criminal Code could be examined from the perspective of restricting some of these common law powers, but I haven't thought this through seriously.

Mr. James Bezan: When you're looking at the use of facial recognition technology and protecting charter and privacy rights, should we take the same approach as we do for wiretaps?

I know the CSE and CSIS do a lot of monitoring of online chatter, trying to focus on things like terrorism and transnational criminal organizations. Again, they can't do indirectly what they're prohibited from doing directly. Whenever they're going to be in violation of the charter, they have to get a warrant or ministerial authorization to ensure that they become charter compliant. When you talk about authorized purposes, is that what you had in mind? Do there need to be warrants or ministerial authorizations making the claim that it is required and proportionate to the violation that may happen to an individual's rights?

● (1210)

Mr. Daniel Therrien: It is conceivable that warrants may be required in some cases. When we recommend that legislation define "allowable" and "prohibited" uses, we have in mind categories of circumstances, such as serious crime, however parliamentarians may want to define it. It's that kind of thing. It's not a case-by-case authorization.

We come closer in our recommendations when we say that there should be "program-level authorization or advanced notification before use". That's closer to Quebec legislation, whereby a police body would come to an independent regulator and say they want to use FRT in the following use case—not an individual circumstance, but a group of cases—which would then be discussed with the data protection authority and approved at the program level. That's closer to individual authorization.

It's not inconceivable that, in some cases, individual warrants would be issued by a judge for an individual case, but that's not our starting point.

The Chair: Thank you, Mr. Bezan.

Ms. Thompson, thank you for joining us today at the ethics committee. Welcome.

Please go ahead for up to five minutes.

Ms. Joanne Thompson (St. John's East, Lib.): Thank you, Mr. Chair. I'm delighted to be here.

My question is for the Privacy Commissioner, Mr. Therrien.

Earlier today, you referenced a moratorium. I believe you indicated that you would support this around the use of facial recognition technology by law enforcement until the regulatory framework around the technology is in place. Would you elaborate on that, if indeed you would be in support of such a moratorium?

Mr. Daniel Therrien: Our starting point as commissioners—me and my provincial and territorial colleagues—is that the law should ultimately define "allowable" and "prohibited" circumstances for the use of FRT, facial recognition. That's because we are of the view that there are compelling circumstances in which that technology should be usable by police forces. I would not be in favour of a complete ban of the technology, because it does allow use in compelling circumstances.

In my reference to the RCMP, I was suggesting that short of the legislation we truly hope will be adopted in the not too distant future, if the RCMP were to undertake to use that technology only according to a policy—and the RCMP representative last week identified certain characteristics of that policy as being "targeted, time-limited", etc.—that would be a voluntary partial moratorium, if I may use that expression.

With regard to a complete ban on facial recognition until a new law is adopted, I would not be in favour of such a ban.

Ms. Joanne Thompson: Thank you.

Would this apply to the use of facial recognition in public spaces as well?

Mr. Daniel Therrien: Yes, the recommendations that we are making would apply to public spaces as well.

Ms. Joanne Thompson: I'd like to move on to personal information protection in electronic documents. I have had a lifetime of working in this area.

Currently it's technology neutral, which allows it to endure over time. Should a technology-neutral law apply to facial recognition technology?

Mr. Daniel Therrien: We're back to the question that I answered a few minutes ago.

Principles-based, technology-neutral legislation for the private sector makes sense as a starting point. The reason we're recommending that there be specific legislation for police forces has to do with the harms of that particular technology of facial recognition. It may well be that certain uses of the technology by private companies raise extremely high risks, not only to privacy but to other rights. Clearview is a good example. We call that mass surveillance.

Mr. Fergus referred to other circumstances. I agree that to denote emotions in order to sell a product, or for whatever other purpose, should not be allowed.

We will provide a few examples of good pieces of legislation. There's draft legislation in the European Union, not yet adopted, which is a good model. Obviously, it would have to be adapted. It says, among other things, that facial recognition should not be used to violate human rights That applies horizontally, whether to the state or to private companies. That is something that I think Canadian parliamentarians should seriously consider.

● (1215)

Ms. Joanne Thompson: Thank you.

One of the threads that I keep coming back to in the conversation this morning is how we align the realities of the speed of the technology around facial recognition with the need to methodically establish the legislation and the protection around human rights, security and privacy. How do you create that balance?

Mr. Daniel Therrien: It is through principles-based legislation, augmented—when need be, given the context—by more specific legislation.

I will add this. I heard you ask certain witnesses at this committee if it's too late. It's never too late. Actually, the fact that certain practices are currently occurring should be no reason for you to prevent yourself from doing the right thing and regulating the technology in a way that respects the rights of Canadians.

We are living, not completely but in part, in a world of self-regulation that has led to certain unacceptable practices. It's not because they are routine or banal, as my colleague Diane Poitras would say, that they should continue to be authorized.

The Chair: Thank you, Commissioner.

In keeping with the day here, were tacking on about an extra 35 or 40 seconds to each person's round.

Go ahead, Mr. Villemure. You're next, for two and half minutes or so.

[*Translation*]

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

A number of studies we've looked at lack conclusive data, but there is nevertheless the possibility of determining things like people's sexual preferences and political opinions, and making such distinctions possible. Are we talking about an unreal world or do we need to look into this matter in the near future, Mr. Therrien?

Mr. Daniel Therrien: There's nothing unreal about it, and the legislation put forward in Europe, which I just mentioned, is designed to prohibit such practices, because they constitute a genuine risk already.

Mr. René Villemure: It's a fascinating tool for making distinctions.

We've also heard about biometric terrorism, which is the corruption of databases as people enter and leave the country, to facilitate criminal behaviour. Have you had anything to do with this type of information, not necessarily at the commissioner's office, but in your research generally?

Mr. Daniel Therrien: Can you give us a little more detail about terrorism? Are you talking about people who might want to enter the country by falsifying data?

Mr. René Villemure: Would it be possible to facilitate someone's entry by changing all the biometric data so that someone could enter under a false identity? Can the biometric data be falsified at the entry and exit points for criminal purposes?

Mr. Daniel Therrien: It's not impossible. That gets us back to the idea of protections on the use of facial recognition. Extremely tight security is needed to prevent such risks.

Mr. René Villemure: All right.

Ms. Poitras, you said earlier that people had not given consent in the Clearview AI case, but all our witnesses have told us that such consent would be impossible to obtain for the use of mass facial recognition. What would you suggest in this regard?

Mrs. Diane Poitras: That's a good question, because obtaining consent from people in the context of facial recognition is not always appropriate.

First of all, there is a power asymmetry, whether between the citizen and the state or the citizen and a major corporation, like the web giants.

Secondly, it's difficult to give informed consent, which is one of the essentials of consent. It's an extremely complex technology, and a citizen's ability to give informed consent is, in my view, very limited. The way to mitigate the consent issue consents is to legally authorize some uses, such as some of the recommendations made today. One could also prohibit certain forms of utilization, where it is believed that even with consent or authorization, its use would not be appropriate in a democratic society. I believe that if acceptable and unacceptable ways of using the data were to be set out in the legislation, it would be a step in the right direction.

● (1220)

[*English*]

The Chair: Thank you.

Now we have Mr. Green.

Mr. Matthew Green: Thank you, Mr. Chair.

You will know we have spent quite a bit of time trying to begin to understand facial recognition technology, yet I believe AI offers perhaps an even more expansive way in which public sector and private sector interventions in our day-to-day lives are rapidly shifting our social context. I think about *Minority Report*. I think about the police's rhetoric around proactive policing and their ability to do predictive policing.

My questions are to the Information and Privacy Commissioner of Ontario, who participated in the process that led to a policy on the use of artificial intelligence technologies by the Toronto Police Services Board by providing comments on the draft policy prior to public consultation.

Were the recommendations you made to improve the draft policy reflected in the final policy?

Ms. Patricia Kosseim: Certainly all of our consultations with the Toronto Police Service, including the oversight board, tend to be highly constructive. I point specifically to our consultation, for instance, on body-worn cameras, which resulted in an overarching framework that has since been published.

With respect to the artificial intelligence framework they developed recently, and their policy, we were consulted. We made a number of recommendations, not all of which were adopted, and we continue to consult with them in the development of the procedures.

Mr. Matthew Green: Just to be clear on that, which ones of importance would you note today were not adopted by the TPS?

Ms. Patricia Kosseim: If I may, Mr. Chair, I would like to ask Vance Lockton. He did the analysis and compared our recommendations with the ultimate policy.

Mr. Vance Lockton (Senior Technology and Policy Advisor, Office of the Information and Privacy Commissioner of Ontario): Thank you.

I wouldn't say there's anything important that wasn't adopted within the policy that can't be adopted within the procedures.

There was a lot of discussion about getting better definitions of risk levels or a better understanding of how some of the oversight was actually going to happen. We have accepted that it's understandable that this high-level policy may not have it, but it's going to be important to see in the procedures that implement that policy.

Mr. Matthew Green: Mr. Chair, I'd like to ask this to all members who are present today. I'm very interested in finding out what their analysis is on artificial intelligence—and maybe they can perhaps provide it in writing to the committee—as it relates to the shifts in ideologically motivated violent extremists and the way in which algorithms and social media are impacting the social context. I reference the recent disruptions here in the nation's capital and other instances across the country.

Thank you.

The Chair: Thank you.

Now we have Mr. Bezan for five minutes.

Mr. James Bezan: This is a question for all three commissioners.

I think there's an understanding that there are certain times we want to use FRT for police enforcement. Is the way those images are harvested, such as scraping social media, something that should be banned?

Mr. Daniel Therrien: That's the issue we looked at in Clearview. If you're within a category or circumstance in which the police should be able to use facial recognition and rely on the technology of a private sector partner, we think the police should ensure the private sector partner has acted lawfully. To scrape social media data from the Internet regardless of the privacy settings of a consumer, for instance, would not be lawful. Even for a serious crime, that should not be possible.

● (1225)

Ms. Patricia Kosseim: I agree.

I would simply add that mass surveillance is the area that caused us the greatest concern on behalf of all federal, provincial and territorial commissioners. Whether it would be done by a third party private sector company on behalf of the police service or the police service itself, this is an area we've highlighted in particular as worrisome.

Mr. James Bezan: Madam Poitras, would you comment?

[*Translation*]

Mrs. Diane Poitras: I don't have anything to add to what my two colleagues have said. Mass surveillance can indeed be carried out by police forces and private companies, in all sorts of ways, including digital surveillance, but that ought not to be the case.

[*English*]

Mr. James Bezan: Are there any clear examples of charter rights being violated in FRT-based prosecution of individuals in Canada?

Mr. Daniel Therrien: I'm not aware of such a case, no.

Mr. James Bezan: Are there examples in Ontario?

Ms. Patricia Kosseim: I'm not aware of any either.

It will be a long time before we get to the point where there is jurisprudence under the charter. This was the concern we had, and it was the reason we were motivated to recommend the adoption of a legislative framework and, in the interim, the development of guidelines to help mitigate risks.

Regarding charter jurisprudence, it may take several years before we see the results.

Mr. James Bezan: Are there examples in Quebec?

[*Translation*]

Mrs. Diane Poitras: I don't have any examples to give you.

[*English*]

Mr. James Bezan: I appreciate the four recommendations to move forward with legislation and the guidelines that Ontario is proposing. Commissioner Kosseim, we really do appreciate that input.

Part of this is going to come under the Privacy Act and PIPEDA, but when you start talking about common law and statute law used in criminal cases, I'd like to know where in the Criminal Code we are going to make these amendments on using FRT so that it can be charter compliant.

Mr. Daniel Therrien: I'll go back to one of your earlier questions.

If, in certain circumstances, warrants would be required to be issued by a court, then we're probably in a world where these amendments would be made through the Criminal Code. I haven't given a whole lot of thought to the overall instrument. It's important for the law to be adaptable, and therefore principles-based, and to determine allowable and prohibited uses. If you want to get into mechanics such as warrants, then perhaps the Criminal Code would be warranted.

To add to what my colleague Commissioner Kosseim was saying about the evolution of the law, which takes time, we currently have a patchwork of laws that govern facial recognition. We have the charter at the highest end. We have the common law. We have certain statutes, including privacy legislation, but we also have other laws. It's a complex web of laws.

We have not seen many examples of the use of the technology, but through the use of Clearview by the RCMP, we have seen that the use of the technology by police forces is sometimes questionable.

My point is that you have to act fairly quickly, because in the meantime, this patchwork of laws can be used in many ways.

● (1230)

The Chair: We'll now move on to Ms. Saks for five minutes.

Ms. Ya'ara Saks (York Centre, Lib.): Thank you, Mr. Chair.

Thank you to all of our witnesses today. This has been a really informative process of learning.

I'm happy to have all three witnesses answer.

Each of you has talked about the need for strong, independent oversight powers of audit when it comes to the processes that use FRT technology, particularly law enforcement. We had a brief time with the RCMP and the TPS last week, and they talked about risk evaluation and terms of use.

What are the mechanisms or proposed recommendations regarding who determines the risk level to justify use? I'm pleased that there are recommendations today, but the details on how that would be done are pretty thin. The risk assessment could be on an immediate-needs basis. It's almost as if we'd be assessing whether use was justified after the fact.

Perhaps Mr. Therrien can start.

Mr. Daniel Therrien: We're back to the complexity of how to craft the law.

Let's say we're within the realm of a serious crime, which, according to our recommendations, would lead to the police being able to use facial recognition. The law cannot know of all individual cases, so there will have to be, as you say, a risk management assessment made by a police force.

What is the conversation with the oversight body, including privacy commissioners? I think it starts with a conversation before the program is put into place—a privacy impact assessment. How are you going to assess risk in a category of circumstances?

Then, if the police want to develop a program, we say that there should be program-level authorization. The police describe the program, which is, say, the protection of very important people in public spaces. That's the program. There's a discussion between the police and the Privacy Commissioner on that program. That's before the use of the technology. Once the technology is adopted and actually used, oversight should include the authority to investigate complaints and make orders as to the lawfulness of the use of the technology in a given case.

Ms. Ya'ara Saks: Thank you.

Just stepping off on that, on the issue of transparency, when there's a risk assessment done and the level of risk determines that FRT would be used, do you feel that there should be public transparency in this, whether it's in law enforcement or...? We'll get into commercial settings shortly.

Anyone can answer.

Ms. Patricia Kosseim: Thank you for the question.

Directly to your latter question, we do believe that a certain level of transparency is absolutely critical. We understand that transparency is not going to be possible with every specific use, but certainly it should exist at the programmatic level, including in privacy impact assessments—if not in their entirety, then at least as a summary of the privacy impact assessments.

To your earlier question about oversight, I think there are multiple ways of achieving that oversight short of a comprehensive legislative review. That includes the role of the boards that play an important oversight role, the data protection authority of that jurisdiction, including my office and my colleagues, and also the public. The Ontario Human Rights Commission, for instance, in my jurisdiction, played an important role in consultation with us and others in the development of a body-worn camera program that was adopted.

I think there's a multilateral consultation process that needs to take place in determining the spectrum of risks. I want to make a point that I think we've made several times, which is that there is a great spectrum of use cases, including administrative uses of facial recognition that may be on the acceptable side of the spectrum and may be adopted.

● (1235)

Ms. Ya'ara Saks: Thank you.

I know that I'm going to be short on time and I want to make sure I get this in.

Madame Poitras, I apologize that the question is in English; I'm just simply more comfortable.

You talked about consent, particularly when it comes to commercial use and so on. For example, Cadillac Fairview and other companies operate public spaces, but they're private property spaces.

What kinds of mechanisms could we consider for operating and managing FRT in those spaces in terms of making sure the public is informed?

The Chair: Could we have a very brief answer, please?

[*Translation*]

Mrs. Diane Poitras: Thank you, Mr. Chair.

Once again, I think that the mechanisms can be tailored to the circumstances. There are different forms of facial recognition. There is facial recognition proper, whose purpose is to identify individuals. However, the term “facial recognition” is sometimes used to designate derivatives of the technology that can be used for corporate purposes, in shopping centres for example, where the goal is not to identify individuals, but rather their characteristics, like age, sex, time spent window shopping…

[*English*]

The Chair: I'm going to have to stop there. We're way over time now. I think we can maybe time this nicely, hopefully, with the expected bells and our final round of questioners.

First we have Mr. Villemure.

[*Translation*]

Mr. René Villemure: Do I still have two and a half minutes left, Mr. Chair?

The Chair: Yes.

Mr. René Villemure: Thank you.

Mr. Therrien, a little earlier, you mentioned the efforts made by the European Commission. Did these include private corporations or only government organizations?

You're indicating both. Okay.

Can your guidance document provide useful ideas for private corporations as well?

Mr. Daniel Therrien: [*Inaudible—Editor*] and adapted to the context.

Mr. René Villemure: Yes, of course.

At the moment, do you know of any entities that are neither commercial nor governmental, but possibly criminal, that use facial recognition?

Mr. Daniel Therrien: We don't have any intelligence on that.

Mr. René Villemure: Okay. Thank you very much.

Ms. Poitras, I'd like to ask you the same question.

Do you know of any entities that are neither commercial nor governmental, and possibly criminal, that use facial recognition?

Mrs. Diane Poitras: I don't have any information on that.

Mr. René Villemure: Thank you very much.

Mr. Therrien, would you go so far as to say that we could learn from the current work being done by the European Commission on facial recognition?

Of course, the context would have to be taken into consideration, but is their work in the forefront at the moment?

Mr. Daniel Therrien: The purpose of the legislation is to protect constitutional rights and human rights. So from that standpoint, the answer is yes, definitely. As to whether it's the best model, I'm not sure whether my colleagues would all agree with me, but I would say that it's a very good model.

Mr. René Villemure: What do you think about this, Ms. Kosseim?

Ms. Patricia Kosseim: Excuse me, but I didn't understand which model you were talking about.

Mr. René Villemure: I'm talking about the European Commission's work.

Do you think we can learn from it, or use it as a model for our work?

Ms. Patricia Kosseim: Absolutely. It's a good model and we can certainly learn from it.

Mr. René Villemure: Thank you very much.

What do you think about it, Ms. Poitras?

Mrs. Diane Poitras: It's unanimous. We can certainly learn a lot from it and adapt it as required.

Mr. René Villemure: The General Data Protection Regulation, the GDPR, was also a good model for the protection of privacy.

Mr. Therrien, in the time I have remaining, do you have any final comments to make?

Mr. Daniel Therrien: Facial recognition is a technology which, when used improperly, can very seriously violate basic rights. I've heard questions about the desirability of a flexible principles-based act. It's generally true, but in view of the consequences of facial recognition, I would strongly encourage you to go beyond principles and to provide specific provisions.

Mr. René Villemure: Thank you very much.

[*English*]

The Chair: Thank you.

For the final round of questions, we go to Mr. Green for two and a half minutes or so.

Mr. Matthew Green: Thank you.

I go back to this notion of private sector use of AI and third party use of AI with law enforcement. There have even been allegations of political use in some cases.

My question, through you to the Information Commissioner, is this: Has there been, within your mandate, the ability to explore or study the use of private sector AI for nefarious things like citizen surveillance, phone hacking and this sort of thing?

● (1240)

Mr. Daniel Therrien: Nefarious by...?

Mr. Matthew Green: Well, I'll give you an example.

There was a lawsuit about NSO's Pegasus. It was used to hack into phones of people who were critical of the State of Israel. We've seen that technology used in different ways. We know that Clearview is one particular thing, but there's certainly Cambridge Analytica and others. What has your office done to provide some kind of understanding about the nefarious use of artificial intelligence as it relates to threats to national security?

Mr. Daniel Therrien: I would go back to my general point. Yes, we have investigated the link between Facebook and Cambridge Analytica. We have studied the use by Cambridge Analytica of data, in some cases to try to influence political processes. There can be also other nefarious uses.

I think it's high time to stop looking at privacy as a technological issue for the very few and to look at the use of technology particularly when it collects personal information for the link of these technologies with fundamental rights, and to legislate accordingly.

Mr. Matthew Green: Mr. Chair, in wrapping up, I look forward to the opportunity to perhaps expand on that and referencing elections that are coming up with regard to allegations that have gone on through various troll farms and different types of social interventions that have happened.

I don't know that we'll have the time to deal with it this time around—

The Chair: You have a bit of time. Ask another question.

Mr. Matthew Green: Okay.

Do we have the ability within existing legislation to adequately account for that private sector influence politically within our social context?

Mr. Daniel Therrien: The rules are too vague to give the necessary level of trust that citizens should have in the collection of information by many parties, including the public sector and the private sector. I think the government recognizes that there's a need to enhance trust.

At this point, people use technology because it's convenient. Frankly, there's no other way to live in modern times than to use technology, but people do it with not much trust, and it is high time for elected officials to regulate these various areas.

Mr. Matthew Green: Thank you for that testimony.

Thank you, Mr. Chair.

The Chair: Thank you. You timed that perfectly. The bells are now ringing, so I'm going to adjourn the meeting. We've had four complete rounds, so I think we're ready to adjourn and attend the votes in the House of Commons.

Thank you very much to all three of our witnesses. It was very informative. Once again, thanks.

The meeting is adjourned.