HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

44th PARLIAMENT, 1st SESSION

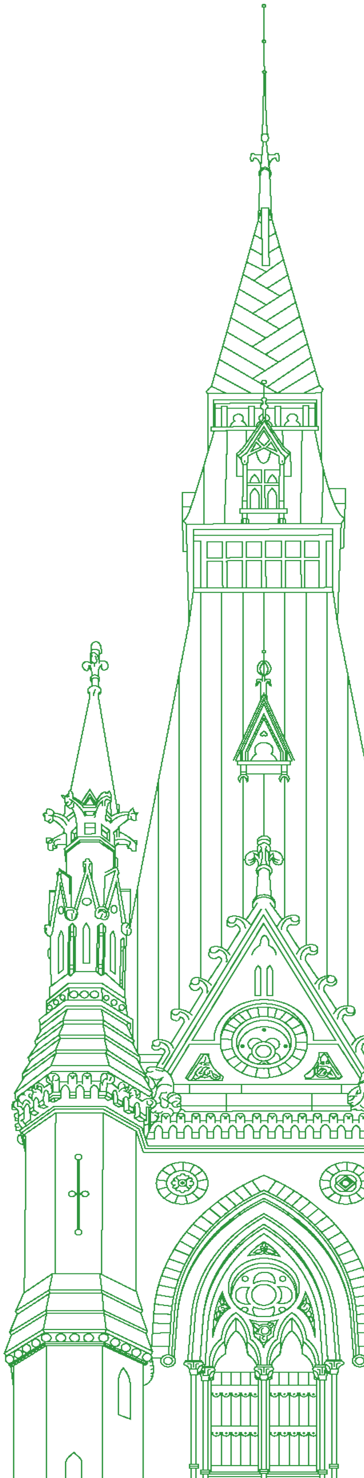
Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 019

PUBLIC PART ONLY - PARTIE PUBLIQUE SEULEMENT

Thursday, May 5, 2022



Chair: Mr. Pat Kelly

Standing Committee on Access to Information, Privacy and Ethics

Thursday, May 5, 2022

● (1535)

[*Translation*]

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

Welcome to meeting number 19 of the House of Commons Standing Committee on Access to Information, Privacy and Ethics.

[*English*]

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. Members are attending in person in the room and remotely by using the Zoom application.

I have a couple of comments for the benefit of witnesses. We have witnesses in the room and witnesses participating by Zoom. Please wait until I recognize your name before speaking. If you are participating by Zoom, click on the microphone icon to activate your mike, and please mute yourself when not speaking. In the room, your mike should be controlled—you shouldn't have to hit the button—but just be aware and make sure that your microphone is lit up before you speak. I'll remind you that comments should be addressed through the chair.

Now I would like to welcome our witnesses.

We have, from Microsoft, Owen Larter, director responsible for artificial intelligence public policy; and from the National Council of Canadian Muslims, we have Mustafa Farooq, chief executive officer; and Rizwan Mohammad, advocacy officer.

We will start with Mr. Larter.

You have up to five minutes for your opening statement.

Mr. Owen Larter (Director, Responsible Artificial Intelligence Public Policy, Microsoft): Thank you very much.

[*Translation*]

Good afternoon, everyone.

[*English*]

Thank you very much, Mr. Chair and vice-chairs, for the opportunity to contribute today.

My name is Owen Larter. I'm in the public policy team in the Office of Responsible AI at Microsoft.

There are really three points that I want to get across in my comments today.

First, facial recognition is a new and powerful technology that is already being used and for which we now need regulation.

Second, there is a particular urgency around regulating police use of facial recognition, given the consequential nature of police decisions.

Third, there is a real opportunity for Canada to lead the way globally in shaping facial recognition regulation that protects human rights and advances transparency and accountability.

I want to start by applauding the work of the committee on this really important topic. We at Microsoft are suppliers of facial recognition. We do believe that it can bring real benefits to society. This includes helping secure devices and assisting people who are blind or with low vision to access more immersive social experiences. In the public safety context, it can be used to help find victims of trafficking and as part of the criminal investigation process.

However, we are also clear-eyed about the potential risks of this technology. That includes the risk of bias and unfair performance, including across different demographic groups; the potential for new intrusions into people's privacy; and possible threats to democratic freedoms and human rights.

In response to this, in recent years we've developed a number of internal safeguards at Microsoft. They include our facial recognition principles. It includes the creation of our Face API transparency note. This transparency note communicates in language that is aimed at non-technical audiences how our facial recognition works, what its capabilities and limitations are and the factors that will affect performance, all with a view to helping customers understand how to use it responsibly.

Facial recognition work builds on Microsoft's broader responsible AI program. This is a program that ensures colleagues are developing and deploying AI in a way that adheres to our principles. The program includes our cross-company AI governance team and our responsible AI standard, which is a series of requirements that colleagues developing and deploying AI must adhere to. It also includes our process for reviewing sensitive AI uses.

In addition to these internal safeguards, we also believe that there is a need for regulation. This need is particularly acute in the law enforcement context, as I mentioned. We really do feel that the importance of this committee's work cannot be overstated. We commend the way in which it is bringing together stakeholders from across society, including government, civil society, industry and academia to discuss what a regulatory framework should look like.

We note that while there has been positive progress in places like Washington state in the U.S., with important ongoing conversations in the EU and elsewhere, we do believe that Canada has an opportunity to play a leading role in shaping regulation in this space.

We think that type of regulation needs to do three things. It needs to protect human rights, advance transparency and accountability, and ensure testing of facial recognition systems in a way that demonstrates they are performing appropriately.

When it comes to law enforcement, there are important human rights protections that regulations need to cover, including prohibiting the use of facial recognition for indiscriminate mass surveillance and prohibiting use on the basis of an individual's race, gender, sexual orientation or other protected characteristics. Regulations should also ensure it's not being used in a way that chills important freedoms, such as freedom of assembly.

On transparency and accountability, we think law enforcement agencies should adopt a public use policy setting out how they will use facial recognition, setting out the databases they will be searching and how they will task and train individuals to use the system appropriately and to perform human review. We also think vendors should provide information about how their systems work and the factors that will affect performance.

Importantly, systems must also be subject to testing to ensure they are performing accurately. We recommend that vendors of facial recognition like Microsoft make their systems available for reasonable third party testing and implement mitigation plans for any performance gaps, including across demographic groups.

We also think that organizations deploying facial recognition must test systems in operational conditions, given the impact that environmental factors like lighting and backdrop have on performance. In the commercial setting, we think regulation should require conspicuous notice and express opt-in consent for any tracking.

I'll close my remarks by saying that we commend many of the elements of the provincial and federal privacy commissioners' recommendations from earlier this week, which set out important elements of the legal framework for facial recognition.

Thank you very much.

● (1540)

The Chair: Thank you, Mr. Larter.

Now we have Mr. Farooq for five minutes.

Mr. Mustafa Farooq (Chief Executive Officer, National Council of Canadian Muslims): I'll actually pass it over to my colleague, if that's okay, Chair.

The Chair: Okay, Mr. Mohammad, go ahead.

Mr. Rizwan Mohammad (Advocacy Officer, National Council of Canadian Muslims): Thank you, Mr. Chair and members of the committee, for the opportunity to offer our thoughts on this study.

My name is Rizwan Mohammad, and I'm an advocacy officer with the National Council of Canadian Muslims, the NCCM. I'm joined today by NCCM CEO Mustafa Farooq. I'd also like to thank NCCM intern Hisham Fazail for his work on our submission.

Today we want to look at the heart of the problem with facial recognition technology, or FRT. A number of national security and policing agencies, as well as other government agencies, have come before you to tell you how FRT is an important tool that has great potential use across government. You've been told that FRT can help escape problems of human cognition and bias.

Here are some other names that you all know, names affiliated with times that these same agencies told you that surveillance would be done in ways that were constitutionally sound and proportionate. The are Maher Arar, Abdullah Almalki and Mohamedou Ould Slahi.

The same agencies that lied to the Canadian people about surveilling Muslim communities are coming before you now to argue that while mass surveillance will not be happening, FRT can and should be used responsibly. Those agencies, like the RCMP, have already been found to have broken the law according to the Privacy Commissioner when it comes to FRT.

We are thus making the following two recommendations, and we want to be clear that our submissions are limited to exploring FRT in the non-consumer context.

First, we recommend that the government put forth clear and unequivocal privacy legislation that severely curtails how FRT can be utilized in the non-consumer context, allowing only for judicially approved exceptions in the context of surveillance.

Second, we recommend that the government set out clear penalties for agencies caught violating rules around privacy and FRT.

Let us begin with the first recommendation, calling for a blanket ban on FRT across the government without judicial authorization in the context of any and all national security agencies, including but not exclusive to the RCMP, CSIS, and the CBSA. You know the reasons for this already. A 2018 report in the U.K. found new figures showing that facial recognition software used by the U.K. Metropolitan Police returned incorrect matches in 98% of cases. Another study from 2019, which drew on a different methodology, reported that the Metropolitan Police returned incorrect matches, or a false positive rate, in 38% of cases.

We are well aware that FRT works differently, and with different accuracy results, depending on the technology, but we all acknowledge as a matter of fact that there are algorithmic biases when it comes to FRT. Given what we know, given the privacy risks that FRT poses, and given that Canadians, including members on other committees in this House, have raised concerns around systemic racism in policing, we agree with other witnesses who have appeared before this committee in calling for an immediate moratorium on all uses of FRT in the national security context and for the RCMP until legislative guidelines are developed.

Simultaneously, we recommend that in developing legislative guidelines, a very high threshold be utilized, including judicial authorization, oversight and timeline limitations.

Secondly, we are shocked by the blasé attitude that the RCMP has taken in approaching the issue of its use of Clearview AI. First the RCMP denied using Clearview AI, but then confirmed it had been using the software after news broke that the company's client list had been hacked. An excuse was given that the use of FRT wasn't known widely in the RCMP. The false answer the RCMP gave to the Privacy Commissioner, which was as credible as the “dog ate my homework” excuse, was completely unacceptable.

The RCMP then had the audacity, after the Privacy Commissioner's findings in the report, to state that it did not necessarily agree with the findings. While the RCMP has taken certain steps to ameliorate the concerns raised, a failure of accountability, when it comes to clear errors and misleading statements, must require clear penalties. Otherwise, how can we trust any such process or commitment to avoid mass surveillance?

We encourage this committee to recommend that strong penalties be assessed against agencies and officers who may breach the rules created around FRT, potentially through an amendment to the RCMP Act. We will provide the committee with a broader written brief in due course.

Subject to any questions, these are our submissions.

Thank you.

● (1545)

The Chair: Thank you for those remarks.

We will begin our questions with Mr. Williams. Mr. Williams, you have six minutes.

Mr. Ryan Williams (Bay of Quinte, CPC): Thank you to our witnesses for attending today.

Through you, Mr. Chair, I have some questions for Mr. Larder.

There's knowledge that you banned U.S. police services from using facial recognition technology. What was the situation, or what were the actions taken, that led Microsoft to ban those police services from FRT?

Mr. Owen Larter: Thank you very much for the question.

It is the case that we don't sell facial recognition to local police in the U.S. I think our position is that it's really important to get law in place that can protect human rights in the context of facial recognition. I think one of the challenges in the U.S. is that there is no law on that front. There isn't any privacy law, the type of privacy law that you have in a lot of other countries, including in Canada, although I'm aware of ongoing conversations around how the privacy framework in Canada can be improved and that they are important conversations to have as well.

That's our position. That's why we're using our voice proactively, to attend conversations like this and contribute to important work like this to make sure that we can get in place some robust regulation for the use of facial recognition, with particular urgency around police and more broadly to make sure that the technology is being used in a way that is transparent, accountable and rights-protecting.

Mr. Ryan Williams: Are Canadian police services also banned?

● (1550)

Mr. Owen Larter: That's not the policy at present.

Mr. Ryan Williams: Is that because we have different policies here? Are there policies that Canada has right now that you like?

Mr. Owen Larter: Yes. To come back to what I referenced before, I think there's a framework of laws that we're looking for to ensure that facial recognition is used in a way that is rights-respecting. I think privacy law is a part of that. I think there's an opportunity to improve privacy frameworks around the world. We're aware of the ongoing conversation in Canada as well. The lack of any sort of broad privacy laws in the U.S. is the main reason for that position.

Mr. Ryan Williams: Thank you.

You just talked about how your responsible AI had a set of guidelines that had to be followed for its use. What are those guidelines?

Mr. Owen Larter: We have our broader responsible AI program, which we have been developing for the last few years. It has a few components. We have a company-wide AI governance team. This is a multi-stakeholder team with some of our Microsoft researchers. These are world-leading AI researchers sharing knowledge about where the technology is and around where the state-of-the-art technology is going. They come together with people working on legal and policy issues and people with an engineering background to oversee the general program.

In terms of the other components, we also have a responsible AI standard. This is a set of requirements across our six AI principles, which I can go into detail on, that ensure that any teams that are developing AI systems or deploying AI systems are doing so in a way that meets our principles.

The final piece we have is also a “sensitive use” review process. This comes into play when any potential development or deployment of a system hits one of three potential triggers. Any time a system is going to be used in a way that affects an individual's legal opportunities or legal standing, any time there is a potential for psychological or physical harm, or any time there is an implication for human rights, then the governance team that I mentioned will come together and review whether we can move forward with a particular deployment or development of AI to ensure that it's being done in a responsible way.

You can imagine that those conversations apply across all of our systems, including the discussions we're having on facial recognition.

Mr. Ryan Williams: Thank you.

You talked about proper testing protocols. What recommendations would you make to our committee on what you're using for proper testing protocols? Do they use also human review in terms of looking at that technology?

Mr. Owen Larter: We think that this is a really important part of the conversation, and it's for a number of reasons.

The accuracy of facial recognition has improved markedly in recent years. There's some very good research being done by the National Institute of Standards and Technology in the U.S., or NIST, that shows that accuracy has improved markedly for the best-performing systems in recent years. There is, however, a very wide gap between the best-performing systems and the least well-performing systems, and the less accurate systems tend to be more discriminatory as well, so we think testing is really important.

There are a couple of components to it. We think that vendors like Microsoft should allow for their systems to be tested by independent third parties in a reasonable fashion, so we allow for that at the moment via an API. A third party can go and test our system to see how accurate it is. We think that vendors should be required to respond to any testing and address any material performance gaps, including across demographics, so that's one thing: vendors doing something on the testing side.

We also think it's really very important that organizations deploying a facial recognition service test it in operational conditions. If you are a police customer and you're using a facial recognition system, you shouldn't just take the word of the vendor that it's going to be accurate in the abstract; you also need to test it in operational conditions. That's because environmental factors like image quality or camera positions have a really big impact on accuracy.

You can imagine that if you have a camera that is placed looking down on someone's head and there are smudges on the lens or poor quality imagery going into the system in general, it's going to have a really big impact on performance; therefore, there should also be a testing requirement for organizations deploying facial recognition to make sure that they know that it is working accurately in the environment in which it's going to be used.

Mr. Ryan Williams: Thank you very much, Mr. Larter.

The Chair: Now, for six minutes, we have Ms. Hepfner.

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

Thank you to all the witnesses for joining us today. I'd also like to start with you, Mr. Larter.

I was reading an article written by Microsoft's Brad Smith in 2018 that covers a lot of issues similar to those you are talking about today. Facial recognition technology was being developed, and Microsoft was calling on government to impose regulations on the industry.

I'm wondering if you could reflect on how it works when tech giants can come up with this technology and then ask governments to regulate it. Is that how it should work? Are there better ways that we can maybe bring governments in as technology is being developed?

I'm just hoping you can reflect on that a bit.

● (1555)

Mr. Owen Larter: It's a really important question, and we definitely think that it's for government to play a leading role in creating a regulatory framework for technology in general, including technologies like facial recognition.

We've tried to do a couple of things over the last few years. First was to implement internal safeguards so that we're doing our bit as a vendor of facial recognition to make sure that the technology is being used responsibly. I talked about our responsible AI program. We also have our Face API transparency note, which I think is a really important part of the conversation and hits at this need for transparency around how facial recognition is developed and deployed.

This transparency note is a document that we make publicly available, and it is clear about how a system works in terms of some of the capabilities of the technology, limitations about the technology and what it shouldn't be used for and the factors that will affect performance, so that a customer using the technology is well informed and able to make informed and responsible deployment decisions.

That's some of what we've been doing internally. We do also think—because it's really important to build trust in technology in general and particularly in facial recognition, given some of the potential risks it can raise, which I mentioned in my remarks—that there is also a need for a regulatory framework.

We are keen to support those conversations. That's why we're very happy to be invited to discussions like this today. We really want to contribute our knowledge around how the technology works and where it is going so that we can create, led by governments and in conjunction with others across society like civil society, a good, robust regulatory framework for technology so that the benefits of this powerful technology can be realized in a way that also addresses some of the challenges.

Ms. Lisa Hepfner: Thank you.

In your opening remarks, you went over a bunch of different ways that FRT is being used for good reasons and for possibly bad reasons as well. Can you let this committee know, through you, Mr. Chair, how widespread FRT is in our society right now? How is it affecting the lives of everyday Canadians?

Mr. Owen Larter: It's a very good question. I would say it is increasingly used. It is a technology that can have a lot of benefits, and I think individuals and organizations are realizing that.

There are a few different applications. A lot of them have to do with security, such as verification using facial recognition. For example, when you're logging in to your phone or your computer, often that is done through a facial recognition tool now. Frictionless and contactless check-in at airports would be another example of how facial recognition is being used, which has been particularly important over the last couple of years during the depths of the COVID crisis, obviously.

Beyond that, I think there are some really beneficial applications in the accessibility context. There are a number of organizations doing really interesting research around how you can use facial recognition to help those who are blind or with low vision better understand and interact with the world around them. We had a project called Project Tokyo, which involved facial recognition, and it used a headset so that a blind individual would be able to scan a room—let's say a canteen or an open space at work—and if there was someone who had enrolled in the system and consented to be part of this individual's facial recognition system, he or she would be able to identify that person and be able to go over proactively and start a conversation in a way that would be very difficult otherwise.

Another application that I think a lot of people in the accessibility community are excited about is facial recognition for people with Alzheimer's or similar diseases that make it increasingly difficult to remember or recognize friends and loved ones. You can imagine the way in which facial recognition is now being explored to help prompt individuals to be able to recognize those friends and loved ones.

It's becoming a long answer, but I'll round off by saying there are also positive applications in the law enforcement context as well. We do think that as part of the criminal investigation process, facial recognition, with robust safeguards around it, can be a useful investigative tool. It's also being used for online identification of missing and trafficked individuals, including children, in a way that has been very beneficial as well.

There are some real benefits there, but, again, there are the challenges that I also mentioned, which is why you need a regulatory framework that can realize those benefits in a way that addresses the challenges.

● (1600)

Ms. Lisa Hepfner: Thank you very much.

Mr. Chair, I have about 30 seconds left. I would just like to give this committee oral notice of a motion that I distributed yesterday. It is as follows:

> That, pursuant to Standing Order 108(3)(h)(vii), the committee undertake a study in order to examine the issue of digital surveillance by employers of Canadians who work from home, including: (a) the prevalence of digital surveillance by employers; (b) the types of surveillance being collected; (c) how personal surveillance data is being stored and secured; (d) what rules are in place to protect employees' privacy rights while working from home; (e) data collection disclosure and permission rights of employees; that the committee report its findings and recommendations to the House; and that, pursuant to Standing Order 109, the committee request that the government table a comprehensive response to the report.

Thank you.

The Chair: Thank you. You are giving notice of this motion?

Ms. Lisa Hepfner: I'm giving oral notice. Thank you.

The Chair: We received this, so it was....

Ms. Lisa Hepfner: I'm just putting it on the record. Thank you very much.

The Chair: Indeed. Thank you.

[*Translation*]

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

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

My questions will be for Mr. Larter.

Mr. Larter, you said that Microsoft does not sell its technology to law enforcement. Does Microsoft have military agencies, surveillance agencies, or intelligence agencies as clients?

[*English*]

Mr. Owen Larter: We do think that facial recognition can have applications in the security and law enforcement context. I think what's really important to note here is that we take a risk-based approach to how we assess using a system and the kinds of customers that we will work with.

We have our sensitive use review process that I mentioned, with those three triggers. Anytime we're going to deploy a system—whether it's facial recognition or something else—in a way that will hit one of those three triggers, we go through a robust sensitive use review process.

We do make our facial recognition available for law enforcement and security uses. We think technology can have some useful applications in those scenarios, but it's really important that there be robust safeguards around that use, including the internal safeguards I've mentioned at Microsoft, but also a regulatory framework that ensures that we're all clear on how the technology is being used and know that it's being used in a way that is trustworthy and responsible.

[*Translation*]

Mr. René Villemure: Could you, at a later date and in writing, provide the committee with examples of the safeguards in question?

[*English*]

Mr. Owen Larter: Yes, for sure. I would be very happy to do that.

[*Translation*]

Mr. René Villemure: That's fine. Thank you very much.

The question may seem strange to you, but is Microsoft looking for this to be regulated so that later they can say they even advocated for a framework, and it's okay if certain things happen?

It may seem irrelevant, but does having such a framework protect Microsoft?

[*English*]

Mr. Owen Larter: It protects Microsoft to have a framework in place, but not necessarily for the reasons that were mentioned. We generally think that it's really important to build a regulatory framework for technology in general that engenders trust and shows that technology is being used in a trustworthy fashion.

We have been around for a while now. We're almost 50 years old as a company, and we realize that if society is going to reap the benefits of technology and if people are going to use it, they need to trust it. Regulation is a really important part of building that trustworthiness framework. That's what we advocate for in general, and that's particularly why we are investing time in trying to advocate robust safeguards around facial recognition, given that it is a very powerful technology with some very positive applications, as I mentioned, but potentially some challenges as well.

Creating a framework around facial recognition that ensures it can be used in a trustworthy way, and in a way the public sees is trustworthy as well, is very important for society so that it can reap the benefits and make sure that this technology is used over the longer term.

[*Translation*]

Mr. René Villemure: I really like your approach, by the way.

We would be grateful if you could send us, afterwards, any information you have on safeguards, types of programs and facial recognition technology liability, or anything related to that.

My next question may seem somewhat surprising to you.

Is there a connection between facial recognition technology and the new metaverse?

[*English*]

Mr. Owen Larter: That's a good question. I would say thank you very much for the invitation to submit materials. We would really appreciate that opportunity. We think the work the committee is doing here is very important, and we want to be as supportive and helpful as possible. I appreciate the opportunity to send some materials, and we will do that.

In terms of the metaverse, everyone is getting very excited about the opportunities there, and I think that is right. There will be a number of technologies that go into creating the metaverse and ensuring that it is performing in a way that people are excited about and is responsible.

I think facial recognition will be one of those technologies, alongside a whole host of other technologies. The metaverse—we call it it the “multiverse” at Microsoft—offers a huge number of opportunities that we're really only just starting to explore as a society. There's a big conversation that we should have around exactly what we want the metaverse to look like and what the safeguards are that we need there to make sure we're reaping the benefits of the technology and addressing some of the challenges.

Facial recognition will definitely be part of that in all kinds of ways that we probably can't even fully appreciate at this point.

● (1605)

[*Translation*]

Mr. René Villemure: Thank you very much for your response. This is a conversation we will probably have in another committee, but it is very interesting.

Could you tell me what industries Microsoft's major facial recognition clients are in?

[*English*]

Mr. Owen Larter: There is a real mix of different sectors. A lot of the applications we use ourselves. These are things like Windows Hello on our Microsoft devices. If anyone has a Surface or a Windows device, Windows Hello is a big part of that.

More broadly, there are a lot of security and verification applications. Particularly banking and aviation have been exploring this type of security approach. We have banking in Australia, for example, that has been exploring using facial recognition to do PIN-less interactions at an ATM. You would just verify yourself with your face at an ATM to withdraw cash.

Those are a lot of the applications. They tend to be around verification and security, getting into devices and such.

[*Translation*]

Mr. René Villemure: Thank you very much.

[*English*]

The Chair: With that, we now go to Mr. Green for six minutes.

Mr. Matthew Green (Hamilton Centre, NDP): My first questions will be through you, Mr. Chair, to Mr. Larter.

Mr. Larter, I'm going to put some questions to you in a rather rapid-fire way. When you hear me say “thank you” as an intervention, it's to take back my time and move on to the next question. Don't take it as a personal affront, but I have an urgency in the way in which I'm going to ask these questions.

I've heard today that you have not banned the use of FRT technology in Canada with law enforcement. Which agencies in the military, the police and law enforcement do you currently have contracts with, both past and present?

Mr. Owen Larter: In Canada?

Mr. Matthew Green: Correct.

Mr. Owen Larter: I am not aware of any contracts at present, but I do want to make sure that I am getting you an accurate answer to that question, so—

Mr. Matthew Green: Mr. Larter, have you had any contracts with the RCMP?

Mr. Owen Larter: I would have to check that. When it comes to facial recognition, I don't believe so, but I would have to go and check that.

Mr. Matthew Green: Mr. Larter, just for the record, you're the director of public policy in the Office of Responsible AI at Microsoft. If you were to have contracts with law enforcement locally here in Canada, as the director, would that have gone past your desk? Would you have been made aware of those contracts? Would you have had to authorize and sign off on them?

Mr. Owen Larter: Yes, I wouldn't have had to authorize them and sign off on them, but there definitely would have been conversations from across the company, including the wider team that I am a part of, the Office of Responsible AI, which likely would have been involved in that, but—

Mr. Matthew Green: Thank you very much.

In your statements, you stated that you did have contracts—i.e., it's not banned in Canada, because I think you stated that you thought we had sufficient legislation in place, a framework that would have been more robust than in the States. I'll give you the opportunity now, as the director of public policy, to perhaps offer with specificity which parts of our privacy and PIPEDA laws you think warrant the use for this, should your company have contracted with law enforcement, the military and the other agencies, as suggested.

Mr. Owen Larter: Yes, I think there are a couple of bits to it. There are the internal safeguards that I mentioned, including the sensitive use review process. Any deployment of technology with the kinds of clients you're talking about would have gone through that sensitive use review process to make sure that we were—

Mr. Matthew Green: Internal to Microsoft?

Mr. Owen Larter: [*Inaudible—Editor*]

Mr. Matthew Green: Yes, but that would have been the same in the States, wouldn't it?

Mr. Owen Larter: Yes, exactly. That's—

Mr. Matthew Green: So why the difference in policy, sir?

Mr. Owen Larter: Because it's on a case-by-case basis. In Canada we would be looking at any deployment to make sure that it was being done robustly. I would say—

Mr. Matthew Green: Yet in a market the size of the United States of America, Mr. Larter, you have banned it. You're waiting for a regulatory framework. This whole committee was in fact set up because we don't have, arguably, a regulatory framework, and we've heard that in previous testimony.

I am asking you, as the director of public policy for responsible AI at Microsoft, why there is the double standard between this market and the market in the States.

● (1610)

Mr. Owen Larter: Yes, it's an important question, and we don't see it as a double standard.

The reason we're here today is that we want to play a participatory role in creating facial recognition in general. We think there is a real opportunity in Canada. We do think that in the U.S. in particular there is that lack of any general privacy framework, which is a problem in terms of this framework of human rights protection that—

Mr. Matthew Green: Mr. Larter, I'm going to take back my time. Thank you for that statement. I encourage you to tune in to the rest of the testimony, as you may find that our current frameworks here in Canada aren't actually adequate.

With that, I'll pivot my questions to our friends from NCCM and Mr. Mohammad, who I think had some very salient points in the opening remarks.

Sir, your website states that you've received hundreds of human rights-related complaints from members of the public who feel that they've been discriminated against. In some of my earlier lines of questioning, I likened this use to racial profiling, street checks and likewise. In your view, is FRT being used as a method for racial profiling?

Mr. Rizwan Mohammad: I'd like to invite our CEO to address your question.

Mr. Matthew Green: Sure. We have two minutes, and I have a couple more questions.

Mr. Mustafa Farooq: Thank you very much.

I think the reality is that the answer is yes, we think there is a high possibility of this happening.

The reality is that we get calls all the time, which people don't hear about, from folks who are undergoing surveillance from CSIS, from the RCMP, and the issues that result out of that. The reality is that this is across the sector. We know already that the CBSA pilot-tested a piece of technology called AVATAR at the airports, which was supposed to be a sort of lie detector that's been used and that, by the way, has now been banned in other jurisdictions. We have grave concerns for how this technology can continue to be weaponized to profile people for potential terrorism.

Mr. Matthew Green: Given the nature of your advocacy and work in the community, has your organization received any human rights complaints related to or connected to artificial technology, including the use of facial recognition?

Mr. Mustafa Farooq: Not at this point, but I think in large part that may have to do with the fact that many folks don't necessarily know that they've been caught in these kinds of things. We sometimes hear concerns around people attending peaceful rallies, whether that's in Vancouver or Hamilton or other places. There are pictures being taken by law enforcement. We don't necessarily know what's always being done with those things, but in large part that has to do with the fact that there has been a lack of disclosure.

Mr. Matthew Green: As I recall, quite some work has been done in the community around no-fly lists and the targeting of Muslim-sounding names and profiles. Sometimes those as young as six or eight months old are being put on a list and can't fly.

In your opinion, could this technology be used surreptitiously to provide these same types of racially profiled and targeted acts of discrimination by the government on your community?

Mr. Mustafa Farooq: Absolutely.

Mr. Matthew Green: Thank you very much.

Thank you, Mr. Chair.

The Chair: Thank you. You left him only about two or three seconds to answer, and we got it in under the wire.

With that, we move to the next round of five minutes. It is Mr. Kurek. Go ahead.

Mr. Damien Kurek (Battle River—Crowfoot, CPC): Thank you very much, Mr. Chair, and thank you to our witnesses here today.

Let me start, as I often do, by inviting the witnesses to feel free to submit further documentation to this committee if they, in testimony today, are not able to have an adequate chance to expound on their answers. It is certainly welcome, and it helps us.

Mr. Larter, as an example to frame my question, in the initial design of cameras, the chemicals used were specifically created around the acknowledgement of generally a white person's face. I've done some reading and seen some documentation on that being the case, so there are technical limitations to FRT.

I'm wondering if you can comment on whether Microsoft has taken that into account in the development of its FRT, and on the possible implications that would have specifically when it comes to things like different races, genders, etc.

Mr. Owen Larter: That's a really important question, so thank you for it.

As I mentioned, I do think one of the big risks that need to be addressed through regulation is the potential risk of discriminatory performance in facial recognition technology. Something we've been very mindful of as we've been developing our technology is making sure we have representative datasets that we're training the facial recognition on so that it can perform accurately, including across different demographic groups.

We would say that this is where the testing piece is very important and that you don't just take our word for it. We think it's important that vendors make available their facial recognition for that reasonable, independent third party testing that I mentioned, so that you're able to scrutinize how companies selling facial recognition are doing in terms of the algorithms they are building. That type of scrutiny, I think, is really important in terms of raising the bar—

● (1615)

Mr. Damien Kurek: Thank you. I, like Mr. Green, acknowledge that we have a short amount of time. In about 30 seconds, could you share with this committee the relationship between FRT and artificial intelligence?

Mr. Owen Larter: Yes, sure. Artificial intelligence pertains to a broad range of systems, of which facial recognition is one. Facial recognition is a type of technology that is able to perform human-like observation or human-like recognition. We would class facial recognition as a type of AI alongside a variety of other AI systems.

Mr. Damien Kurek: Thank you very much.

To our friends from the NCCM, we heard you reference needed amendments within the RCMP Act. Are there any other acts that, in your opinion, would need to be amended to ensure that we address some of the challenges that are faced when it comes to things like racial profiling?

Mr. Mustafa Farooq: I think we may want to look at the CSIS Act as well.

Mr. Damien Kurek: Sure.

Mr. Mustafa Farooq: I think the reality is that we still don't know—and to the best of my knowledge, this committee has not been told—whether CSIS uses facial recognition technology. That's a knowledge deficiency Canadians deserve to have the answers to. Depending on those sets of answers, we may also be thinking about what that looks like in terms of penalties for non-disclosure.

Mr. Damien Kurek: We obviously spent a lot of time in this committee on the governmental implications. I'm curious, though, if you have any further thoughts about the private applications. We all use some FRT, probably—I'm making assumptions here—with the face recognition to log into our phones and whatnot. We all use a little bit of FRT in some sense.

Would you have any comments on not just the public implications of the use of this technology but in terms of the private application as well, whether it be on technology like personal electronic devices or otherwise, such as within stores and that sort of thing?

Mr. Mustafa Farooq: Unfortunately, we're not experts in the area of how this could be looked at from a consumer or a corporate perspective, but I will say that there are significant concerns within our communities generally about how large tech companies are taking in this data, how it's being used, and how it's being sold and given potentially to authoritarian regimes. I'm not saying this about any particular tech company, but certainly those are concerns we're hearing broadly from our community.

Mr. Damien Kurek: I know I'm getting very close here, and maybe I'll simply ask you this. You mentioned judicial benchmarks as your suggestion. If you would have further information that you could provide to this committee as to what you feel an appropriate judicial benchmark would be for the application of FRT, for example, in a law enforcement context, certainly this committee would appreciate that. Thank you very much.

With that, my time is up. Thank you to the witnesses.

The Chair: Thank you.

Next we go to Mr. Bains for five minutes.

Mr. Parm Bains (Steveston—Richmond East, Lib.): Thank you, Mr. Chair, and thank you to our guests who are joining us today.

My question is for the gentleman joining us from the National Council of Canadian Muslims.

We've heard from witnesses before this committee that agencies have been using facial recognition technology. You also mentioned in your comments that in places like Vancouver and other parts of the country, if there are rallies or things like that where people are gathered, the technologies are being used. Someone mentioned that the VPD was also using it in British Columbia.

I'm curious about that. To your knowledge, to what level are these agencies using this technology? I will have follow-up questions after that.

● (1620)

Mr. Mustafa Farooq: I wouldn't want to speak on behalf of any particular agency, obviously. To the best of my knowledge, after complaints were brought forward to the Vancouver police specifically, that jurisdiction imposed a moratorium now on FRT technologies.

However, we know that is not a universal standard. When folks say they are doing something, we know that there continue to be concerns around whether they are actually doing it.

Mr. Parm Bains: Thank you.

Have you been engaged by any of these Canadian police authorities about facial recognition technology?

Mr. Mustafa Farooq: Other than very peripheral conversations, no.

Mr. Parm Bains: Have you put forward recommendations for improving Canada's legal framework for governing artificial intelligence technology? Have you made submissions?

Mr. Mustafa Farooq: Other than to this committee, we have put forward nothing formal, other than other concerns around online harm regulation and the role that AI plays in that conversation.

Mr. Parm Bains: Is there a reason you have not been able to engage with these agencies? Have you reached out?

Mr. Mustafa Farooq: Quite simply, it's very hard to engage in a conversation when basic facts aren't being acknowledged.

When CSIS tells us that they're not going to answer a basic question—which is the same question they haven't answered for you right now—about whether facial recognition technology is being used, it becomes very hard to get any sense of accountability. It becomes very hard to have a conversation. When the RCMP tells us one thing, tells Canadians one thing and tells the Privacy Commissioner one thing, it becomes very hard to have a good-faith, honest conversation about what the future could actually look like.

I think all of us are interested in a world in which law enforcement uses facial recognition technology responsibly. Folks are right when they say that there are potential good-use cases, especially in child pornography and cases like that. The reality is that our agencies here are simply not meeting the standard that Canadians expect them to, for all of the reasons that you all know about, vis-à-vis systemic racism and so many of these other challenges.

Mr. Parm Bains: Thank you.

If I have time, I have a quick question for Mr. Larter.

Several witnesses have raised concerns that facial recognition technology has been shown to misidentify racial individuals more often than white individuals. We've heard that on numerous occasions here in this committee. How does your organization address that risk?

Mr. Owen Larter: That's a really important question, and it's one of the major risks that we think needs to be addressed around facial recognition use.

I'll come back to what I said before in terms of the internal safeguards we've mentioned. One of the most important is the testing piece. We make sure that we are opening up our facial recognition system to independent third party testing to make make sure that we are training and testing it ourselves in such a way that we are confident it is performing accurately and in a way that minimizes gaps across different demographic groups.

I would really like to emphasize as part of my contribution today that the testing piece is a really important part of making sure that technology is performing in an accurate manner, which it can do. It's made incredible strides in the best-performing algorithms in recent years, but there are many algorithms out there that aren't as accurate. You need to be able to test them to make sure that when, for example, police are using them, they are using the most accurate systems.

The Chair: Thank you.

Mr. Parm Bains: Thank you. Do I have any more time?

The Chair: I'm afraid, Mr. Bains, that you are out of time.

We'll go now to Monsieur Villemure for two and a half minutes.

[*Translation*]

Mr. René Villemure: Mr. Larter, I will turn to you again. Since we only have two and a half minutes, let's be brief.

For Microsoft, what constitutes surveillance?

[*English*]

Mr. Owen Larter: I guess surveillance would be observing individuals or groups.

[*Translation*]

Mr. René Villemure: Is that with or without their consent?

[*English*]

Mr. Owen Larter: It could be done without their consent, and that would problematic. I think it could be done with their consent. In large part, you would think of surveillance being done perhaps without an individual's consent.

[*Translation*]

Mr. René Villemure: When we know that, sometimes, facial recognition can indicate—not all studies support this—a person's political or sexual preferences, in a way, we can say that there is no more freedom possible. We are monitored at all times.

● (1625)

[*English*]

Mr. Owen Larter: I think these are real concerns that need to be addressed. Again, that's why we're advocating regulation.

I think we're skeptical about some of the claims around what facial recognition can do—like intuit an individual's political beliefs just by looking at that person—so I think a conversation around regulation that identifies those uses that are permitted, and also, importantly, those uses that are not permitted, is a really important thing to have.

[*Translation*]

Mr. René Villemure: In the absence of regulation in Canada, at this time, is Microsoft under contract with any Canadian government agency, security, surveillance or intelligence agency?

[*English*]

Mr. Owen Larter: Did you ask if Google or Microsoft...? Sorry.

[*Translation*]

Mr. René Villemure: I'm talking about Microsoft, obviously.

[*English*]

Mr. Owen Larter: Not to my knowledge, no, not that I'm aware of—not with facial recognition in Canada.

[*Translation*]

Mr. René Villemure: So you don't work with any government agencies, security agencies, military organizations or surveillance agencies.

[*English*]

Mr. Owen Larter: To my knowledge, we're not.

[*Translation*]

Mr. René Villemure: Do you trade in data? I am talking about both buying and selling them.

[*English*]

Mr. Owen Larter: Not in relation to facial recognition, necessarily. We wouldn't sell any data we're using in relation to our facial recognition systems. That would be my answer.

[*Translation*]

Mr. René Villemure: Thank you.

[*English*]

The Chair: Thank you.

We'll go next to Mr. Green for two and a half minutes. After that, we will have another round, just to be clear. We'll make sure we have a full hour with these witnesses.

Go ahead, Mr. Green, for two and a half minutes.

Mr. Matthew Green: Thank you.

Through you, Mr. Chair, to Mr. Larter, I alluded to this, but I want to make sure that there's 100% clarity in my ask.

Mr. Larter, I'm asking you and requesting that for the purpose of this study in this committee, you provide this committee with a list of all contracts, both present and past, related to our public safety—government-related, military-related, law enforcement and police agencies in Canada—given that you were unable to provide that testimony here today. Do you understand that request?

Mr. Owen Larter: I do. To my knowledge, we don't have any contracts to that effect, but I understand the request.

Mr. Matthew Green: Thank you very much. I do appreciate that.

Through you, Mr. Chair, to Mr. Farooq, I believe I heard in your opening comments, Mr. Farooq, some talk around legislative reforms. I want to underscore my perception of where we're at in this country with testimony we've heard previously from our other guest witness and ask if you have contemplated within your submission, with specificity, different ways in which we can tighten up our framework to ensure that we have knowledge of the use, that we have accountability of the use and that it's done in a way that is in accordance with our charter rights.

I'm just wondering if you can expand on any of your earlier comments about some of the legislative improvements you feel we should make.

Mr. Mustafa Farooq: Absolutely, and thank you for this very important question.

We will provide a longer exploration in a brief submission, but what I would say in general is, first of all, that I think the banning of real-time FRT in places like airports and our borders is important as we think about a general categorization.

In terms of investigative tools, while we're calling for a moratorium until these policies are developed, we think the set-up should be very similar to how it works when the police are trying to obtain any search warrant: that they appear before a judge and they put forward their argument and their best-case scenario, with clear documentation, which is then provided to the public. We'll provide specific submissions on the sections and subsections that we think need to be amended.

Mr. Matthew Green: Thank you very much, Mr. Chair, and thank you to the witnesses.

The Chair: Thank you.

Next we go to Mr. Bezan for five minutes.

Mr. James Bezan (Selkirk—Interlake—Eastman, CPC): Thank you, Mr. Chair, and I apologize that I'm not with you guys in person today. I'm dealing with overland flooding in the riding, and in my own yard.

First I want to direct my questions to Mr. Farooq and Mr. Mohammad. I want to drill down deeper, because as we go forward in this regulatory process, I want to make sure that we check all the boxes of which legislation we need to focus in on.

You've already mentioned CSIS and the RCMP. You've also talked about the Criminal Code amendments that are going to have to happen, as well as Privacy Act and PIPEDA. I know that under national defence, the CSE is mainly listening in on online chatter. Maybe it has the formula we need, because for it to listen to any Canadian or to any of our Five Eyes allies, it can't do indirectly what you're not allowed to do directly. It has to get warrants or ministerial authorizations for issues surrounding national security and national defence.

Is that what you're suggesting are the steps we need to take to ensure the charter rights of Canadians are protected?

● (1630)

Mr. Mustafa Farooq: First of all, we're all hoping that you're doing okay and that your neighbours and everyone else are doing okay.

Mr. James Bezan: There's a lot of water around here, I can tell you that.

Mr. Mustafa Farooq: Generally, if the question is whether we think that as it has been legislatively set out, the standards for obtaining warrants should be similarly applied to FRT in investigative contexts, then there are a couple of slight nuances that need to be done. Generally, the answer is yes, there should be a judicial—

Mr. James Bezan: What are the nuances, then?

Mr. Mustafa Farooq: The nuances come in to some extent when looking at section 8, search and seizure. There would be a bundle of evidence that would go before a judge. That's where things would kick into play.

Mr. James Bezan: Some of the testimony that we've heard from policing agencies was that Clearview AI was doing a lot of the facial recognition technology for police agencies across Canada, including the RCMP and the CBSA. They are no longer using it, because Clearview said that it no longer is offering the service to Canadian agencies.

However, have you ever heard of IntelCenter Check? It also has FRT, and I'm under the impression that it may have contracts with the RCMP, and potentially CSIS.

Mr. Mustafa Farooq: I've heard just what's public, what's been published publicly about them, but I've no specific knowledge.

Mr. James Bezan: We're looking at checks and balances, so first of all we're talking about charter rights and making sure that the legislation covers that through numerous different statutes that we're going to have to amend. The issue comes down to the built-in bias, as many of our colleagues have alluded to, that everything was always developed around facial recognition with white faces, so brown and black faces are seeing a lot of discrepancies and inaccuracies. As has been suggested by different intel companies, police agencies are going to put more human interaction into that process.

Would that satisfy the concerns that your community and others may have here in Canada?

Mr. Mustafa Farooq: Is the question whether more human interaction would ameliorate the problems of FRT? Am I understanding that correctly?

Mr. James Bezan: That's what I'm asking. There would always have to be a human check on anything that FRT and AI would suggest as a person of interest.

Mr. Mustafa Farooq: Respectfully, I actually don't think that would be entirely sufficient.

The reality is that while of course human checks are important, we also know that there is a problem of systemic racism and bias within our police agencies. I don't think that human checks would be fully sufficient. We think that the courts are the place to get those checks and balances, with clear information. How much FRT is being used by a given agency? How is that data being stored? Timelines of destruction of data should be provided to you as parliamentarians. We think that's really important.

The Chair: Thank you.

Now we will go to Ms. Khalid for five minutes.

● (1635)

Ms. Iqra Khalid (Mississauga—Erin Mills, Lib.): Thanks, Chair. I'll go to Mr. Larter first.

Mr. Larter, NCCM today proposed a moratorium on facial recognition technologies. What does your organization think about a moratorium for non-commercial uses of FRT?

Mr. Owen Larter: We think there's definitely the need for regulation, as we've been advocating today. We would suggest investing time and resources in creating that regulation. It takes a lot of time and investment to get any initiative progressed, so focusing on creating regulation, starting with law enforcement uses, is what we would suggest.

I think we would also suggest taking an incremental approach to regulation in this area. It is the case that the technology is developing rapidly. It has improved markedly in recent years. Starting with regulation of law enforcement use, which is the most acute need as we see it, would be what we'd recommend, and investing time and effort into that rather than on advancing a moratorium. That would be our suggestion.

Ms. Iqra Khalid: Thank you.

Mr. Farooq, do you agree with what Mr. Larter is saying?

Mr. Mustafa Farooq: Respectfully, I think we may have a difference of opinion on this question.

Given the potential risks posed to Canadians through FRT, and given the fact that unfortunately our law enforcement agencies have not been appropriately forthcoming, we think a moratorium is appropriate in the non-commercial context. That's the same position that other witnesses who have appeared before this committee have taken. That would be until the full privacy and context regulations can be developed.

Ms. Iqra Khalid: Thank you.

You've outlined how difficult it is to get an open and transparent answer from law enforcement agencies across all levels. How would you propose that a moratorium would specifically be implemented, and how would it be enforced?

Mr. Mustafa Farooq: I think that there are a number of measures. Of course, I think it would require potential regulatory or statutory change.

We would be happy to provide a more extensive answer in terms of precise suggested legislative language in our written brief as well.

Ms. Iqra Khalid: Thank you. I would appreciate that.

Mr. Larter, your company does business all across the world. Are you aware of any states that are using FRT in surveilling their populations?

Mr. Owen Larter: My apologies; the lighting in my room appears to have gone out. I hope people can still see and hear me properly.

I think there are definitely a number of countries across the world that are using facial recognition, particularly non-democratic countries, to surveil their populations in ways that I don't think any of us would necessarily think are positive. We don't engage in that type of activity to help with that type of surveillance approach.

Ms. Iqra Khalid: If you are able to, we'd love to have you identify what some of these countries are and how exactly they are surveilling.

The second thing is that you're a big proponent of regulation of FRT. Are you a proponent of any regulation that you see across the world that you think Canada should adopt, in terms of ensuring that facial recognition technologies are used appropriately not only in the non-commercial sector but also in the commercial sector as well?

Mr. Owen Larter: Yes. I think there have been some positive developments at the state level in the U.S.

Washington state is one to which I would draw the committee's attention. There is a law that went into effect, as of July last year, that lays out some important transparency and accountability measures. It provides for the testing that I mentioned, and it provides, very importantly, for the human oversight piece as well, ensuring that any system output is reviewed by an individual before a decision is made, and makes sure that individual is appropriately trained to do so.

Washington state is certainly one that I think is worth looking at.

Ms. Iqra Khalid: Chair, how much time do I have?

The Chair: You have 25 seconds.

Ms. Iqra Khalid: In that sense, then, I will give a verbal notice of motion:

> That, notwithstanding the motions adopted by the committee on December 13, 2021, and on January 31, 2022, concerning the regular scheduled meetings of the committee regarding the production of reports this spring, given the substantial matters brought forward in the course of our deliberations on facial recognition technologies, the committee extend its hearings on the study of facial recognition by three meetings, and that the committee commence consideration of a report in September 2022.

● (1640)

The Chair: Thank you, Ms. Khalid.

Again, I think we got that on notice, and there are other motions that were placed on notice today as well, but thank you for that.

With that, we will go next to Mr. Villemure for two and a half minutes.

[*Translation*]

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

I will once again address Mr. Larter from Microsoft.

Mr. Larter, you will excuse my pugnacity, but I am very interested in what you are doing.

Is it possible that criminal entities, a foreign power, or some third party could infiltrate and falsify data obtained using artificial intelligence?

[*English*]

Mr. Owen Larter: It's a good question.

I think there's definitely a need for robust cybersecurity around technology in general. Microsoft is making significant investments on that front to ensure that the variety of technologies we provide are secure and that our customers remain secure. There are certainly threats that we all need to be mindful of in ensuring that technology is developed and used—

[*Translation*]

Mr. René Villemure: To your knowledge, have there ever been such security breaches in Microsoft technologies anywhere in the world?

[*English*]

Mr. Owen Larter: My focus is more on the AI systems piece and using it responsibly, so this is a bit outside my area of expertise. However, I think there's always the threat of malign actors, so I think responding robustly and with significant investment, which is what we are doing, is the right thing to be doing.

I'm afraid I can't give much more of a specific answer than that because this is sort of outside the area that I have a focus in.

[*Translation*]

Mr. René Villemure: Thank you very much.

If you could provide this information by consulting with your colleagues, we would appreciate it.

What do you think should be the boundaries of facial recognition?

[*English*]

Mr. Owen Larter: I think this is a fundamental question as part of the regulatory discussion. I think deciding what is a permissible use and what is not a permissible use is very important.

We have some suggestions on this front. We think that indiscriminate mass surveillance is not something that should be permitted. We also think that discriminating against an individual on the basis of race, gender, sexual orientation or other protected characteristics should be prohibited.

Also, the democratic freedoms piece, which we discussed today, is really important, and I'm pleased to hear that it's part of the discussion. That is one to address as well in making sure that the technology is not used in a way that undermines fundamental freedoms like freedom of assembly. I think those are some core uses that we would suggest.

One that is maybe more specific to the law enforcement context as well is that we think it's important that the output of facial recognition is not used as the only reason or the only piece of evidence to take a material decision—for example, to arrest someone.

The Chair: I'm going to have to move on. We're significantly over time for Mr. Villemure.

We will now go to Mr. Green for the final questions.

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

I think Ms. Khalid, in her line of questioning, raised a very important point as it relates to creating a legal framework, and that is what I'll call “the duty of candour” from our security agencies, police, military and CBSA in how they're using these.

Through you, Mr. Chair, to Mr. Farooq, I want to note an August 31, 2021, Globe and Mail report on the court admonishing CSIS once again for the duty of candour. They noted some other cases in which breaches had occurred in the way they sought warrants and the way in which they sought to surreptitiously surveil Canadians unlawfully, quite frankly.

Through you, Mr. Chair, to Mr. Farooq, in your experience, doing the advocacy work that you do—because now we're on the human side of the application of the tool—could you perhaps share with us instances in which our security and public safety agencies may not have been forthcoming about the way in which they were surveilling members of the Muslim community?

Mr. Mustafa Farooq: Sure. I think that the pre-eminent most recent case of relevance for this committee was a decision of Justice Gleeson from the Federal Court about a year and a half ago. This was a stunning decision by Justice Gleeson, wherein he essentially eviscerated CSIS for a persistent habit of trying to mislead the court. Most of us recall that line, but as lawyers, we call it “breaching the duty of candour”. This has been a habit that has been noted not just by Justice Gleeson, but as well by Justice Mosley at the Federal Court in other sets of decisions.

Eventually the director of CSIS, David Vigneault, came forward to say yes, there may have been problems, but stunningly—and I think we've been clear on the record about this—and unfortunately this government chose to appeal that decision, which is still before the courts. I think it's a question of what we are actually going to do to challenge our national security agencies when they mislead folks that remains an open question.

● (1645)

Mr. Matthew Green: Thank you.

Through you, Mr. Chair, to Mr. Farooq, would it be your opinion that any contemplation of regulating the technical aspects of this must also include corresponding and ethical frameworks for government and law enforcement agencies in order to ensure compliance and full transparency in dealing with these tools?

The Chair: Please answer very briefly.

Mr. Mustafa Farooq: I'm sorry. Would you mind repeating the question?

Mr. Matthew Green: Any contemplation of regulation of the technology within the context of this report ought to carry with it a compliance, oversight and accountability framework for the human actors, including our law enforcement and policing agencies, specifically to ensure the duty of candour.

Mr. Mustafa Farooq: Yes, absolutely.

Mr. Matthew Green: Thank you very much.

Those are my questions.

The Chair: Thank you very much.

My thanks to all of our witnesses today.

With that, I'm going to suspend. We will resume in camera.

I'll ask our witnesses, with our thanks, to leave the room relatively quickly. We will carry on in camera in a moment.

The meeting is suspended.

[*Proceedings continue in camera*]

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