HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

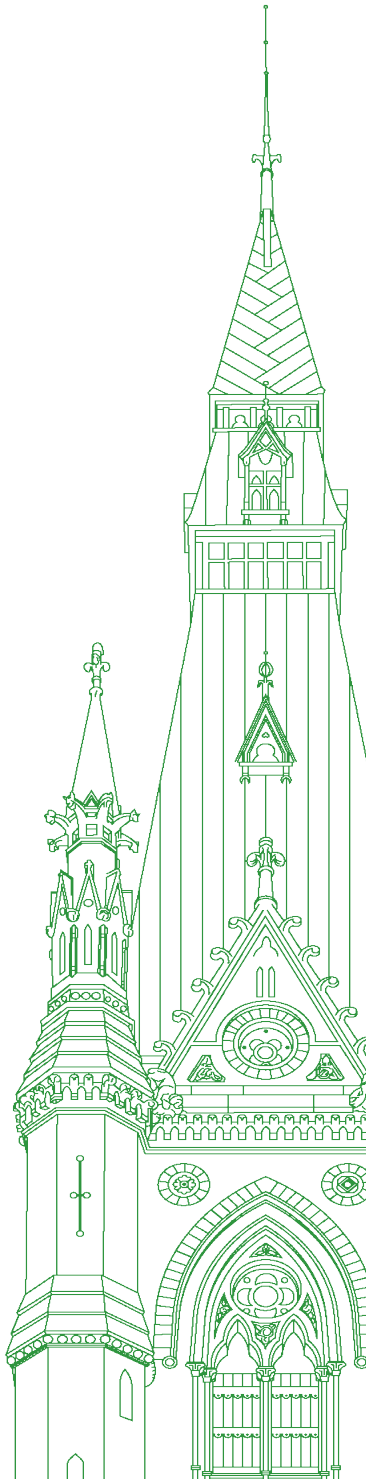
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 012

Thursday, March 24, 2022



Chair: Mr. Pat Kelly

Standing Committee on Access to Information, Privacy and Ethics

Thursday, March 24, 2022

● (1530)

[*English*]

The Chair (Mr. Pat Kelly (Calgary Rocky Ridge, CPC)): Welcome to meeting number 12 of the 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. Members are attending in person in the room and remotely using the Zoom application. So you are aware, the webcast will always show the person speaking rather than the entirety of the committee.

I will remind members in the room that we all know the public health guidelines. I understand that you've heard them many times by now, so I won't repeat them again, but I will ask you to follow them.

I would also like to remind all participants that no screenshots or photos of your screen are permitted. When speaking, please speak slowly and clearly for the benefit of the interpreters. When you are not speaking, your microphone should be on mute. Finally, I would remind you that all comments by members and witnesses should be addressed through the chair.

I would now like to welcome our witnesses today. From Borealis AI, we have Dr. Alex LaPlante, senior director, product and business development. From the Canadian Civil Liberties Association, we have Dr. Brenda McPhail, director of the privacy, technology and surveillance program. From the Computer Research Institute of Montréal, he have Mr. Françoys Labonté, chief executive officer; and from the International Civil Liberties Monitoring Group, we have Mr. Tim McSorley, national co-ordinator.

Just before I turn it over to the witnesses, for the benefit of committee members, what I've tried to do to minimize the time we lose to change over between panels is to run our witnesses in one panel. We will go through the regular rounds of questions and subsequent rounds as time permits in the prescribed formula for speaker allocation.

With that, I turn it over to our first witnesses, from Borealis AI.

Dr. LaPlante, go ahead.

Dr. Alex LaPlante (Senior Director, Product and Business Engagement, Borealis AI): Thank you for the introduction, Mr. Chair.

Thank you to the committee for inviting me to participate as a witness on the topic of the use and impact of facial recognition technology.

As noted, my name is Dr. Alex LaPlante. I am the senior director of product and business development at Borealis AI, which is RBC's R and D lab for artificial intelligence. The views I express today are my own; they do not reflect the views of Borealis AI, RBC or any other institution with which I'm affiliated.

I've spent the last 15 years building and deploying advanced analytics and AI solutions for academic and commercial purposes, and I've seen the positive outcomes that AI can drive. However, I'm also acutely aware that, if we don't take care to adequately assess the application, development and governance of AI, it can have adverse effects on end-users, perpetuate and even amplify discrimination and bias towards racialized communities and women, and lead to unethical usage of data and breaches of privacy rights.

I will focus my comments on two areas: data privacy, and data quality and algorithmic performance. I will then conclude with my recommendations around the governance of this technology.

Biometric data is some of the most sensitive data that exists, so privacy is paramount when it comes to safely collecting, using and storing it. Biometric data has been collected and used without individuals' consent or knowledge in several instances, including in the case of Clearview AI breaching these individuals' privacy rights and putting them at the mercy of unregulated and unvalidated AI systems. This is particularly concerning in high-risk use cases such as criminal identification. There have also been cases of function creep, where companies gain consent to collect biometric data to use in one particular way but go on to use it in other ways beyond this original stated intent.

The best FRT systems can achieve accuracy rates of 99.9% and perform consistently across demographic groups. However, not all algorithms are made equal, and in some cases false positive rates can vary by factors of 10 to even 100 for racialized populations and women. This gap in performance is directly related to the lack of representative, high-quality data.

One field of AI research that should be highlighted in the context of FRT is adversarial robustness. It is the backbone of practices like cloaking, which look to deceive FRTs. This can be achieved through physical manipulation like obscuring facial features or, more covertly, by making modifications to facial pictures that are indiscernible to the human eye but that ensure the pictures are no longer identifiable.

Law enforcement agencies in Canada and abroad have employed technology built on unverified data scraped from the web that can be easily manipulated in ways that are undetectable without direct access to source data. Without proper oversight and regulation, these companies can easily manipulate their data to control who can or cannot be identified with their systems.

Beyond data quality issues, FRT, like any high-risk AI system, should undergo extensive validation so that its limitations are properly understood and taken into consideration when applied in the real world. Unfortunately, many FRTs on the market today are true black boxes and are not available for validation or audit.

While my comments focus on the risks of FRT, I believe there's a lot of value in this technology. We need to carefully craft regulations that will allow FRT to be used safely in a variety of contexts and that address Canada's key legislative gaps as well as concerns around human rights and privacy. In working in the highly regulated financial sector, I have participated in the effective governance of high-risk AI systems where issues of privacy, usage, impact and algorithmic validation are evaluated and documented comprehensively. I believe similar approaches can address many of the primary concerns around this technology.

Regulations need to provide FRT developers, deployers and users with clear requirements and obligations regarding specific uses of this technology. This should include the requirement to gain affirmed consent for the collection and use of biometric data, as well as purpose limitation to avoid function creep. FRT legislation should leverage the privacy principles of necessity and proportionality, especially in the context of privacy-invasive practices.

Further, governance requirements should be proportional to risk materiality. Impact assessments should be common practice, and there should be context-dependent oversight on issues of technical robustness and safety, privacy and data governance, non-discrimination, and fairness and accountability. This oversight should not end once a system is in production but should instead continue for the lifetime of the system, requiring regular performance monitoring, testing and validation.

Last, clearer accountability frameworks for both developers and end-users of FRT are needed, which will require a transparent legislative articulation of the weight of human rights versus commercial interests.

All that being said, these regulations should seek to take a balanced approach that reduces the administrative and financial burdens for public and private entities where possible.

● (1535)

Thank you very much. I look forward to your questions.

The Chair: Thank you very much.

Now we have Dr. McPhail for up to five minutes.

Ms. Brenda McPhail (Director, Privacy, Technology and Surveillance Program, Canadian Civil Liberties Association): Thank you to the chair and the committee for inviting the Canadian Civil Liberties Association to appear before you today.

Facial recognition—or, as we often think of it at CCLA, facial fingerprinting, to draw a parallel to another sensitive biometric—is a controversial technology. You will hear submissions during this study that tout its potential benefits and others that warn of dire consequences for society that may come with particular use cases, especially in the context of policing and public safety. Both sides of the debate are valid, which makes your job during this study especially difficult and so profoundly important. I'm grateful that you've undertaken it.

The CCLA looks at this technology through a rights lens. This focus reveals that not just individual and collective privacy rights are at risk in the various public and private sector uses of face surveillance and analysis, but also a wide range of other rights. I know that you've heard in previous submissions about the serious risk to equality rights raised by faulty versions of this technology that work less well on faces that are Black, brown, indigenous, Asian, female or young—that is, non-white and non-male.

What I'd add to that discussion is the caution that if the technology is fixed and if it becomes more accurate on all faces across the spectrums of gender and race, it may become even more dangerous. Why? It's because we know that in law enforcement contexts, the surveillance gaze disproportionately falls on those same people. We know who often suffers discrimination in private sector applications. Again, it's those same people. In both cases, a perfect identification of these groups or members of these groups who already experience systemic discrimination because of who they are and what they look like carries the potential to facilitate simply more perfectly targeted discriminatory actions.

In addition to equality rights, tools that could allow ubiquitous identification would have negative impacts on a full range of rights protected by our Canadian Charter of Rights and Freedoms and other laws, including freedom of association and assembly, freedom of expression, the right to be free from unreasonable search and seizure by the state, the presumption of innocence—if everyone's face, as in the Clearview AI technology, becomes a subject in a perpetual police lineup—and ultimately rights to liberty and security of the person. There's a lot at stake.

It's also important to understand that this technology is creeping into daily life in ways that are becoming commonplace. We must not allow that growing familiarity to breed a sense of inevitability. For example, many of us probably unlock our phones with our face. It's convenient and, with appropriate built-in protections, it may carry relatively little privacy risk. A similar one-to-one matching facial recognition tool was recently used by the Liberal Party of Canada in its nomination voting process prior to the last federal election. In that case, it was a much more risky use of a potentially faulty and discriminatory technology because it took place in a process that is at the heart of grassroots democracy.

The same functionality in very different contexts raises different risks. This highlights the need for keen attention, not just to technical privacy protections, which exist in both the phone and voting app examples, but to contextually relevant protections for the full set of rights engaged by this technology.

What is the path forward? I hope this study examines whether—not just when and how—facial recognition can be used in Canada, taking those contextual questions into consideration. CCLA believes, similar to our previous witness, that regulation is required for those uses that Canadians ultimately deem appropriate in a fair and free democratic state.

Facial recognition for mass surveillance purposes should be banned. For more targeted uses, at the moment CCLA continues to call for a moratorium, particularly in a policing context, in the absence of comprehensive and effective legislation that provides a clear legal framework for its use, includes rigorous accountability and transparency provisions, requires independent oversight and creates effective means of enforcement for failure to comply.

A cross-sector data protection law grounded broadly in a human rights framework is necessary, especially in the environment where the public and private sectors are using the same technologies but are currently subject to different legal requirements. Better yet, targeted laws governing biometrics or data-intensive algorithmically driven technologies could be even better fit for purpose. There are a number of examples globally where such legislation has recently been enacted or is under consideration. We should draw inspiration from those to create Canadian laws to put appropriate guardrails around potentially beneficial uses of FRT and protect people across Canada from its misuse or abuse.

Thank you. I welcome your questions.

● (1540)

The Chair: Thank you.

Mr. Françoys Labonté, you have up to five minutes. Please go ahead.

[*Translation*]

Mr. Françoys Labonté (Chief Executive Officer, Computer Research Institute of Montréal): Members of the committee, I'm delighted to be participating in this important study.

I'll begin by briefly introducing myself. My name is Françoys Labonté, The Chief Executive Officer of the CRIM, the Computer Research Institute of Montréal. I have a technical background, a PhD specializing in computer vision from the École polytechnique de Montréal. In 2010, I joined the CRIM and became its CEO in 2015. The CRIM has worked on artificial intelligence for many years, almost from the moment it was it established, and had very practical opportunities to work on the development of speech recognition technologies in the 2000s, and on facial recognition in the 2010s.

In keeping with the CRIM's approach, my presentation will be very pragmatic. Right from the outset, it's essential to understand that basically, facial recognition technologies neither require nor involve any personal information. These technologies are limited to showing whether a new image of a face that has never been entered before into a given system matches an image that is already in the system.

In the context of your study, I understand the interest in establishing contexts in which it might be acceptable to link personal information to a face and to be able to identify an individual on the basis of one or more images of that person's face. One of the great challenges for your committee is to strike a proper balance between concerns pertaining to privacy, social acceptability and societal benefits.

We are facing a somewhat paradoxical phenomenon: for many Canadians, one or more images of their face to which their name is directly linked, not to mention other personal information that may sometimes be associated, are already publicly available, whether in social networks, digital media or other digital applications. These images were often supplied by people when they had a particular use in mind, but they agreed to very broad consent clauses and very extensive use rights. Even if someone supplied an image of their face unintentionally, for example to add it to their user profile in a digital application, then in practice it's relatively easy for third parties to access the image and other associated data and to use them with impunity for various other purposes, because the consents obtained are so broad. Practically speaking, it's virtually impossible to reverse the situation and make these images disappear from the Internet, or even to dissociate the personal information linked to them.

Here is a question your committee should look into: given that images of most Canadians' faces, to which their personal information is linked, are publicly accessible, what uses of these images that involve facial recognition ought to be proscribed or strictly circumscribed?

There is probably a strong consensus among Canadians for banning the use of facial recognition technologies in a Big Brother manner, with databases containing images of everyone's face, and public surveillance cameras arbitrarily tracking people's movements and behaviour. Likewise using facial recognition in conjunction with drones in a military context for targeted assassinations would certainly run counter to any initiatives to promote the ethical use of artificial intelligence.

I deliberately want to get you to see things somewhat differently in a context where the answers are probably not so clear-cut and where facial recognition technology is simply replacing or substituting for other existing technologies.

Let's take the example of using facial recognition technology for people in a retail store or a shopping centre. It's easy to draw a parallel with e-commerce which, has gained widespread, though not unanimous, social acceptance. When we shop online in a manner that is considered anonymous, by which I mean that it is not connected to any user account, cookies nevertheless leave behind traces of our time on the web. These cookies are then used to send us advertising on the basis of our preferences. Is that very different from a facial recognition system in a shopping centre, which without explicitly knowing your identity, could on the basis of factors that could readily be inferred from your face or your behaviour, send you targeted advertising?

● (1545)

Similarly, when we shop online, but now by means of a user account to which we have supplied some information…

[*English*]

The Chair: I will have to ask you to wrap up very quickly. You're a little bit over time already.

[*Translation*]

Mr. Françoys Labonté: Right.

Generally speaking, I think people are in favour of using facial recognition technology for specific clearly-stated applications when it's easy to understand the benefits and how the data will be used.

However, there are still enormous challenges to be met in building public confidence and convincing people that facial recognition technology and images will be used properly and only for the purposes that were initially agreed upon.

Thank you.

[*English*]

The Chair: With that, we will go Tim McSorley for the final opening statement, followed by questions by members.

Go ahead, Mr. McSorley.

● (1550)

Mr. Tim McSorley (National Coordinator, International Civil Liberties Monitoring Group): Thank you so much for the invitation and for having me here today, Mr. Chair and committee.

I'm very happy to speak to you today on behalf of the International Civil Liberties Monitoring Group. We're a coalition of 45 Canadian civil society organizations dedicated to protecting civil liberties in Canada and internationally in the context of Canada's anti-terrorism and national security activities.

Given our mandate, our particular interest in facial recognition technology is its use by law enforcement and intelligence agencies, particularly at the federal level. We have documented the rapid and ongoing increase of state surveillance in Canada and internationally over the past two decades. These surveillance activities pose significant risks to and have violated the rights of people in Canada and around the world.

Facial recognition technology is of particular concern given the incredible privacy risks that it poses and its combination of both biometric and algorithmic surveillance. Our coalition has identified three reasons in particular that give rise to concern.

First, as other witnesses today and earlier this week have pointed out, multiple studies have shown that some of the most widely used facial recognition technology is based on algorithms that are biased and inaccurate. This is especially true for facial images of women and people of colour, who already face heightened levels of surveillance and profiling by law enforcement and intelligence agencies in Canada.

This is particularly concerning in regard to national security and anti-terrorism, where there is already a documented history of systemic racism and racial profiling. Inaccurate or biased technology only serves to reinforce and worsen this problem, running the risk of individuals being falsely associated with terrorism and national security risks. As many of you are aware, the stigma of even an allegation in this area can have deep and lifelong impacts on the person accused.

Second, facial recognition allows for mass, indiscriminate and warrantless surveillance. Even if the significant problems of bias and accuracy were somehow resolved, facial recognition surveillance systems would continue to subject members of the public to intrusive and indiscriminate surveillance. This is true whether it is used to monitor travellers at an airport, individuals walking through a public square or activists at a protest.

While it is mandatory for law enforcement to seek out judicial authorization to surveil individuals either online or in public places, there are gaps in current legislation as to whether this applies to surveillance or de-anonymization via facial recognition technology. These gaps can subject all passers-by to unjustified mass surveillance in the hopes of being able to identify a single person of interest, either in real time or after the fact.

Third, there is a lack of regulation of the technology and a lack of transparency and accountability from law enforcement and intelligence agencies in Canada. The current legal framework for governing facial recognition technology is wholly inadequate. The patchwork of privacy rules at the provincial, territorial and federal levels does not ensure law enforcement uses facial recognition technology in a way that respects fundamental rights. Further, a lack of transparency and accountability means that such technology is being adopted without public knowledge, let alone public debate or independent oversight.

Clear examples of this have been revealed over the past two years.

The first and most well known is that the lack of regulation allowed the RCMP to use Clearview AI facial recognition for months without the public's knowledge, and then to lie about it before being forced to admit the truth. Moreover, we now know that the RCMP has used one form of facial recognition or another for the past 20 years without any public acknowledgement, debate or clear oversight. The Privacy Commissioner of Canada found that the RCMP's use of Clearview AI was unlawful, but the RCMP has rejected that finding, arguing that they cannot be held responsible for the lawfulness of services provided by third parties. This essentially allows them to continue contracting with other services that violate Canadian law.

Lesser known is that the RCMP also contracted the use of a U.S.-based private "terrorist facial recognition" system known as IntelCenter. This company claims to offer access to facial recognition tools and a database of more than 700,000 images of people associated with terrorism. According to the company, these images are acquired, just like Clearview AI's, from scraping online. The stigma that comes with being associated with a so-called terrorist facial recognition database only increases the stigma and rights implications associated with it.

As a final example, I'd just say that CSIS has refused to confirm whether or not they even use facial recognition technology in their work, stating that they have no obligation to do so.

Given all these concerns, we would make three main recommendations: first, that the federal government ban the use of facial recognition surveillance immediately and undertake consultation on the use and regulation of facial recognition technology in general; second, based on these consultations, that the government undertake reforms to both private and public sector privacy laws to address gaps in facial recognition and other biometric surveillance; and, finally, that the Privacy Commissioner be granted greater enforcement powers with regard to both public sector and private sector violations of Canada's privacy laws.

● (1555)

Thank you, and I look forward to the discussion and questions.

The Chair: Thank you to our witnesses for their opening statements.

The first round, which will be six minutes, goes to Mr. Kurek.

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

Let me start by sharing a request to all of our witnesses. First, thank you for your expertise and the information that you have shared with us here today. It's very valuable. Certainly as I was preparing for this meeting.... I'm very appreciative of all of you coming to share this with us here today. I know a number of you did make recommendations, and certainly from the practical aspects of what the committee will accomplish in this report, that's very much appreciated.

My ask, beyond a few of the questions that I plan to get to here in a moment, is this: Because there's limited time, if there are further recommendations or information, please feel free to share that with members of this committee so that we can include that information in the report as we compile it in the coming months. Consider that an open invitation, as your expertise here is very much appreciated.

To both Ms. LaPlante and Mr. McSorley, you provided a couple of examples. Clearview AI is one of the most clear examples.

We'll start with Ms. LaPlante.

Are there any other examples that you could briefly share that highlight some of the challenges with these systems?

Dr. Alex LaPlante: Clearview AI is one of the concerning cases. What is so concerning about it is that they have scraped mass amounts of data. It is linked to individuals' identities and this is being used in contexts where the ultimate outcome can be very severe for individuals. I think we have to take this into deep consideration when we're applying AI systems of any kind in those types of contexts.

In terms of other examples of this, Facebook is a really good one. Now they've put this program on hold for a while, but I think all of you are very much aware, if you interact with Facebook, that it used to have a feature that essentially pre-identified a friend who was in a photo. This is directly based on use of your profile information and all of the pictures that you and your friends have posted and tagged. Maybe this is a little bit more of a benign case, and in some cases it could be seen as something that's helpful or convenient, but I also want to recognize that there's a slippery slope in having those types of databases owned by private companies when there is no regulation or oversight for their use.

Mr. Damien Kurek: Thank you for that.

I know I have limited time.

Mr. McSorley, were there any other examples that you could quickly point to that would be worth the committee's time to further look into?

Mr. Tim McSorley: I'd re-emphasize the question of IntelCenter, a U.S.-based company that we know the RCMP contracted with. We have very little information about what they did with that company and with that database.

That's the only other company I can specifically point to, but it adds an extra boost to the concerns that we see with Clearview AI because they use similar tactics, including scraping images online and putting them into a database, but then add the extra stigma of saying that we know these people are associated with terrorism, with absolutely no oversight in terms of how they come to that determination, and then they share it with law enforcement. There's already this stigma attached to individuals with absolutely no reasoning behind it, and then it's used by law enforcement to essentially identify those people as terrorists.

Mr. Damien Kurek: Thank you very much for that.

Ms. McPhail, I really appreciate the comment you made, and I'm paraphrasing here, that improving the tech doesn't actually solve the problem. It's a very important message that needed to be heard here.

We've seen through our work on this committee the importance of operationalizing and defining consent and enshrining things like opt-in and opt-out features that are clear for the public.

Today, in the age of social media and with cameras pretty much being everywhere, how do we as legislators protect Canadians from some of the challenges associated with facial recognition and AI in the space that we're discussing here today?

Ms. Brenda McPhail: Thank you for that question. It's a really important one.

You have to start from the right place. I respectfully disagree with Monsieur Labonté. Facial recognition systems use our face. That is some of the most sensitive personal information we have. Faces are recognized in Canadian privacy law as a piece of personally identifiable information; therefore, they are within the scope of the law.

The best way to protect people across Canada from inappropriate uses of this technology truly is to think through how it needs to be regulated. As a first step, a positive example that this committee might wish to consider is contained in the proposed U.S. Senate bill, Bill S.3284, the ethical use of facial recognition act, which would establish a congressional committee or commission to consider and create guidelines for the use of facial recognition technology in the United States.

● (1600)

Mr. Damien Kurek: I'm almost out of time here, so thank you very much for that. You've written before, and I won't get into the details because of time, but you said “Clearview AI left the Canadian market, but their business model remains.” Are there other examples in our country similar to Clearview AI that this committee should be aware of?

The Chair: Can you do that in about 10 or 15 seconds, please?

Ms. Brenda McPhail: I think that virtually every private sector purveyor of facial recognition technology has a similar model. I would throw your attention towards the Cadillac Fairview mall investigation by the Privacy Commissioner of Canada, which involved a non-consensual private sector use of facial analytics that was deemed appropriate in sort of backroom conversations between a private sector company and their lawyers and was only discovered due to a mistake, a glitch in the technology, that revealed what was happening behind the scenes. Under these kinds of models, almost every facial recognition vendor advertises that it can help private sector bodies leverage personal data to improve their market, and that's a problem.

The Chair: Thank you. We're almost a full minute over time. I'm going to be a little bit less ruthless than I was in the last meeting because of the way we've set this one up. Still I do ask all members of the committee to be conscious of the time when they know they're down to a few seconds and of the questions they pose in that time.

With that said, go ahead, Mr. Fergus.

[*Translation*]

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

In a way, I understand the circumstances for my colleague Mr. Kurec. It's a very thorny issue and we have lots of questions to ask the witnesses. I must admit that I've been doing more and more research into the matter, and every day, the things I've been reading raise further questions.

I'd like to begin by talking about something that Ms. LaPlante mentioned at the outset, and I think that Ms. McPhail raised it as well. It would appear that facial recognition technology is just one facet of our more general concern about the use of artificial intelligence . Some algorithms analyze not only our face, but also our behaviour, the things we say, our voice and how we move.

As a Black Canadian commenting on facial recognition, I am well aware of the fact that cameras cannot render the same image quality for people with darker skin, women or younger people, as for white men. It would appear to be a systemic problem.

Would you agree that the cameras themselves can be prejudicial to some people because they weren't developed specifically for them?

Let's begin with Ms. LaPlante.

[*English*]

Dr. Alex LaPlante: Thank you for your question. It's very interesting and it actually highlights, I would say, some challenges with other technologies that we have. NIST has done very comprehensive studies, and I encourage you to review their reports, in which they have looked at various different aspects of algorithmic performance. Some of those studies have focused specifically on demographics. One issue they have brought up is that data quality is a big driver of algorithmic performance. They've also noted the fact that technologies tend to do quite well for things like mug shots. One reason for that is that mug shot designs are often built in such a way to consider the range of different skin tones. It's more representative of a face. If you have pictures that don't necessarily capture an individual correctly, that will be reflected in the performance of the technology.

● (1605)

[*Translation*]

Hon. Greg Fergus: Thank you for your testimony, Mr. Labonté.

You mentioned the possibility of striking a balance between the concerns raised by these technologies and the benefits of using them.

Is it likely that such a balance can be achieved?

Mr. Françoys Labonté: Of course, the matter of a balance is subjective. I don't know whether I expressed myself clearly. When I said that people made a lot of personal information publicly available, I was alluding to societal behaviour. It does not justify the use of such information for other purposes. As I mentioned, when certain applications use personal information without consent, then clearly that's a problem that has nothing to do with striking a balance.

The example of using Face ID on a telephone was mentioned. This is a highly controlled application that people can use because of its usefulness, in airports for example. I remember that although it was available before the pandemic, people could take pictures of their face to speed up passport checks. It's a very limited context in which images are acquired by the government using a photographic identification process governed by standards. This can [*Technical difficulty*]

Hon. Greg Fergus: We can no longer hear you, Mr. Labonté.

I'll take advantage of this pause to ask Ms. McPhail a final question.

Ms. McPhail, would it be preferable to start from scratch and ban the use of facial recognition for the time being, until a legal framework is developed to specify how it can be used, and under what circumstances?

[*English*]

The Chair: To be clear, Monsieur Labonté, we did lose your audio, and Mr. Fergus had posed another question.

[*Translation*]

Hon. Greg Fergus: I think we've also lost Ms. McPhail.

[*English*]

The Chair: I've also lost your interpretation right now.

We're losing people all over on this call.

We'll suspend the meeting due to technical difficulties.

● (1605)

_____(Pause)_____

● (1610)

The Chair: The meeting is resumed. The Zoom system-wide glitch is hopefully resolved.

I'm going to ask Mr. Fergus to repeat his question, and we'll restart with that.

[*Translation*]

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

My question is for Ms. McPhail.

Ms. McPhail, would it be preferable for the time being to ban any use of facial recognition, whether in the private or public sector, until we can come up with a framework that identifies appropriate uses of the technology? Do you think that would be the best way of proceeding?

[*English*]

Ms. Brenda McPhail: I do. The CCLA has called for a moratorium, which is similar to a ban, until we sort this out, and until we have exactly this kind of conversation with our democratically elected representatives, and people across Canada, to think this through. Are there uses of this technology that are going to benefit us, or are there not? For those that may benefit us, what are the appropriate safeguards to put in place?

That's going to be a long and difficult conversation, but it's an absolutely fundamentally necessary one. A moratorium on the use of this technology would give us the space and time to engage this in a thoughtful, careful, and considered way.

The Chair: Thank you.

With that, Mr. Fergus is out of time.

[*Translation*]

I'll now give the floor to Mr. Garon.

Welcome to the committee, Mr. Garon.

You have six minutes.

Mr. Jean-Denis Garon (Mirabel, BQ): Thank you very much, Mr. Chair.

I'm glad the connection was restored, because I wanted to ask Mr. Labonté most of my questions.

Mr. Labonté, we know that having more information can often lead to better decisions. Nevertheless, more than once in our history, we decided to place limits on our ability to obtain information. For example, I led the effort on searches without a warrant. We prevented the police from conducting searches without a warrant.

I'm wondering whether we are once again pondering a serious social issue, in this instance whether facial recognition technology has the potential to virtually put an end to our freedom and privacy.

What are your thoughts on this matter?

[*English*]

The Chair: Monsieur Labonté.

[*Translation*]

The Clerk of the Committee (Ms. Nancy Vohl): Mr. Labonté, can you hear us?

[*English*]

Mr. Tim McSorley: Excuse me. I have been having trouble hearing the questions in the English interpretation. I'm not sure if others are having the same problem for audio as well.

The Chair: Thank you.

I'll ask the clerk to quickly see if we can establish whether or not we have adequate contact.

The meeting is suspended.

● (1610)

_____(Pause)_____

● (1615)

The Chair: We will resume the meeting.

I would ask the members who are participating virtually to indicate if at any point they lose audio so that I know if there's a problem.

I will restart Monsieur Garon's round, because I don't believe anybody heard his question.

Go ahead. You have six minutes.

[*Translation*]

Mr. Jean-Denis Garon: Thank you, Mr. Chair.

Mr. Labonté, I'm going to repeat the question I just asked.

Gathering more data can lead to better decisions. Nevertheless, more than once in our history, out of concerns pertaining to privacy and individual rights, we decided to restrict information gathering. For example, searches without a warrant are now prohibited.

I am wondering how likely it is that one day, if facial recognition is used inappropriately on a wide scale, it could considerably reduce or even do away with our freedom and privacy. I know that it's a rather philosophical question, but I'd like your opinion on it.

Mr. Françoys Labonté: The answer is yes, I do believe that's possible, if data collection is done without people's consent and without them properly understanding the purposes for which the information is being used. That in fact is what explains recent personal information protection legislation. Questions like these have been on the radar for people working in technology for a long time. Regulations are being implemented, but the questions have been around for a long time. Clear guidelines are definitely required.

On the other hand, there is an important factor to consider from the CRIM's perspective. The CRIM is no longer working on these technologies. The most competitive players at the moment are the ones that collected enormous amounts of data for use in training artificial intelligence models. Now, ordinary mortals no longer have access to the amounts of data required to achieve high performance levels.

It's true, though, that the risk you mentioned is real. That's why it's essential to regulate data harvesting to make people aware of how it is going to be used and to require informed consent.

Mr. Jean-Denis Garon: There are companies like Palantir, which use military technology to produce what they call social observation.

What do you think of these companies and practices?

● (1620)

Mr. Françoys Labonté: It always comes back to the same question. To develop technologies like these, companies collected an enormous amount of data, presumably without the informed consent of the people providing it. It happened. It's a reality. That's what I was saying in a very pragmatic manner in my presentation. Now, some of these players have a significant competitive advantage that needs to be regulated in the future.

What can we do about it? It may be a wide-ranging question, but it's very pragmatic. If we were to ask someone today to return all the images they used to create their models, it would be a challenge for them, because you can't go back in time. That's really the challenge here. We are trying to modulate the future *Technical difficulty*.

Mr. Jean-Denis Garon: Mr. Labonté, you spoke about people who had not consented to supplying their data. We're talking about very complex technologies, the details of which we don't know much about. We don't know what the algorithms are.

Would ordinary citizens be prepared to give their informed consent to allow these companies to use their data?

Mr. Françoys Labonté: Generally speaking, people don't consent to allow a company to use their information any way they want. For example, if someone feels that it's important to allow people to follow them on social media, they consent to make a picture of their face available solely for that purpose, but they would not consent to allow third parties to use the image of their face for profiling or for developing commercial products.

This aspect is dealt with in regulations that are being drafted or that have recently come into force, but it's still very difficult to give informed consent. At CRIM, because it's a research centre, when we work on projects with an ethics committee and ask subjects for consent, such consent is very specific, clear, for a particular purpose, and often for a limited period of time.

In the world today, the speed at which things are happening makes it difficult right now to give informed consent. For example, when people download an application, they don't even read the consent form that accompanies it, or do not understand what it really means.

In fact, giving informed consent…

The Chair: Thank you, Mr. Labonté.

Mr. Green, it's over to you now for six minutes.

[*English*]

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

Welcome to all the guests.

Mr. McSorley, in some of the preliminary research that I have conducted on the brittleness and inconsistencies of facial recognition technology, I've heard it called the modern-day phrenology. Luke Stark equates facial recognition to the plutonium of AI. He states that:

> ...facial recognition technologies, by virtue of the way they work at a technical level, have insurmountable flaws connected to the way they schematize human faces. These flaws both create and reinforce discredited categorizations around gender and race, with socially toxic effects. The second [point] is [that] in light of these core flaws, the risks of these technologies vastly outweigh the benefits, in a way that's reminiscent of hazardous nuclear technologies.

They use that metaphor to say that it, "simply [by] being designed and built, is intrinsically socially toxic, regardless of the intentions of its makers".

In July 2020 the International Civil Liberties Monitoring Group co-signed a letter with OpenMedia asking for the federal government to enact a ban on facial recognition surveillance from the federal law enforcement and intelligence agencies.

Through you, Mr. Chair, to Mr. McSorley, given the inconsistencies, the brittleness and the surveillance capitalism of third parties—

● (1625)

The Chair: I'm just going to interrupt for a moment.

Mr. Matthew Green: I was on a roll.

The Chair: Yes.

You have four minutes and 19 seconds left when we go to time back in, but did I hear a point of order or a question or concern about audio?

Ms. Iqra Khalid (Mississauga—Erin Mills, Lib.): Yes, thank you, Mr. Chair. We did lose it in between there, so I missed about 30 seconds of what Mr. Green had to say.

My apologies, Mr. Green, for interrupting you.

Mr. Matthew Green: I won't start again, but I'll simply ask if Mr. McSorley can give me a thumbs-up that he can hear me at this moment. Perfect.

I will ask through you, Mr. Chair, if he could elaborate on the dangers related to the use of AI technologies like facial recognition by national intelligence agencies such as CSIS and the RCMP for the purpose of mass surveillance. I'll take a specific point of reference that in May 2021 our own Department of National Defence—our military—used technologies to surveil Black Lives Matter in a surreptitious way.

Perhaps Mr. McSorley would like to just comment on its use and on the dangers that I've outlined in my preceding comments.

Mr. Tim McSorley: We would agree completely with your characterization of the dangers posed by facial recognition technology. We see just layers upon layers of concerns.

As has been pointed out by other witnesses today, especially Dr. McPhail, the idea is that there are layers of problems regarding the accuracy of this technology. There are concerns about whether or not we know, without proper regulation, and with so many companies proposing their technology to law enforcement agencies, that they will even be using the most accurate—or will they be using the most accessible, the ones that are targeted more and marketed more towards law enforcement? There's the whole question of the use of law enforcement and intelligence agencies of third party contractors and how that's carried out, the lack of transparency there, and problems with accuracy and bias in the technology that may be promoted to them.

Even if those were to be addressed, as has been mentioned, the targeting of communities of colour is already well known. It cannot be solved simply by improving the technology, but rather, as Dr. McPhail said, it can be exacerbated, because then all of a sudden we have this great tool for better surveilling populations that are already over-policed and over-surveilled. We need to be incredibly—

Mr. Matthew Green: If I may, through you, Mr. Chair, to Mr. McSorley, given the fact that there's been an ongoing theme in this committee and in this study that there are tendencies for the government and for intelligence and security forces to do indirectly what it can't do directly, I'd like to extend the question, because in the same letter that you co-signed, there was a call for reforms to the Personal Information Protection and Electronic Documents Act, or PIPEDA.

Based on your work, what types of reforms are needed to safeguard human rights and privacy in Canada to ensure that third party vendors don't do indirectly what the government can't do directly?

Mr. Tim McSorley: First of all, we need private sector privacy laws that are based on a human rights approach; that are based clearly on proportionality and necessity; that have clear rules around consent; that bring in oversight of artificial intelligence and regulation of artificial intelligence used by the private sector; and also bring in stringent regulations if not bans—it needs to be further studied—on the provision of the use by law enforcement and national security of third party and private contractors in order to carry out those activities that they cannot do themselves.

For example, as I mentioned earlier, the RCMP has disputed that they need to verify the lawfulness of services provided by third party contractors. If the leading federal law enforcement agency in the country says that they can use technology found to be unlawful and that it's not their problem, in so many words, we have a serious problem. That needs to be addressed in the private sector laws just as in the public sector laws, because current private sector laws allow for the sharing of information from the private sector to the public sector in law enforcement because of national security exceptions.

That needs to be a primary focus in reforming Canada's private sector privacy laws.

● (1630)

Mr. Matthew Green: Thank you.

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

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

Thank you to all the witnesses.

I will continue on with Mr. McSorley.

Sir, in June of 2021 you called on the public safety minister to develop a clear proposal for independent oversight of FRT and AI-based policing tools. What is your vision for what the independent oversight would look like?

Mr. Tim McSorley: First of all, we think we need a broader consultation to decide what are no-go zones. As we've said, we believe a clear part of that no-go zone would be on the use of facial recognition for mass surveillance. Beyond that, there needs to be oversight in terms of ensuring that as law enforcement and intelligence agencies adopt new technology, they are reviewed beforehand, before they are implemented, in order to ensure that they meet the right standards that are set by Canada's privacy legislation.

Right now it's up to the law enforcement agencies themselves, essentially, as we've seen with the adoption of Clearview AI, to make those decisions themselves. It wasn't clear that the minister knew to what degree the RCMP was using Clearview AI facial technology. The concern is that it's being adopted without any kind of political or other oversight.

The National Security and Intelligence Review Agency is currently undertaking a review of the use of biometric surveillance by Canada's national security agencies, but that could take, again, a couple of years before it becomes public. We need action by the minister now in order to ensure that we don't have law enforcement adopting these technologies in secret, and that they publicly share what they believe the privacy impact will be through the privacy impact assessments and allow for a full and clear debate.

Mr. Ryan Williams: Your organization wrote an open letter to the minister in 2020. Did you ever receive a response from the minister?

Mr. Tim McSorley: We had a follow-up conversation with the director of policy in the minister's office, but it was more of a listening session rather than clearly stating what the minister's actions would be. The only new information we obtained was clarification that CBSA was not using real-time facial recognition at that moment. They could not share anything about CSIS's use of facial recognition technology, but there was no clear commitment from the minister's office to take further action.

Mr. Ryan Williams: Is it true that in response to some of the findings of the Privacy Commissioner, the RCMP agreed to conduct privacy assessments of third party tools that would establish new oversight function in new technology; and if it's so, has it actually been set up in a way in which it can protect the rights of Canadians?

Mr. Tim McSorley: That's a good question.

We know that the RCMP committed to making improvements to its policies, even though they did reject the overall finding that they're responsible for the lawfulness of third party technology. We haven't seen anything released publicly about that yet, and in fact, it speaks to one of the problems we see right now that, in theory, federal agencies need to undertake privacy impact assessments before new technology or new privacy-impactful projects are undertaken, but those assessments are often not done at all. If they are done, they may be kept secret. There's supposed to be an executive summary shared, but often, especially from law enforcement and intelligence agencies, those aren't shared, based on the idea that it would have an impact on their operations, whereas we feel that there needs to be pressure to have a greater degree of transparency and accountability there.

Mr. Ryan Williams: Okay.

You've answered quite a bit of this already, but I just want to give you a chance to further expand if you'd like. Your third recommendation from the letter was for an establishment of clear and transparent policies and laws regarding the use of facial recognition.

What do you see these policies and laws looking like, and what reforms do you think the Privacy Act and PIPEDA require?

Mr. Tim McSorley: Our expertise is more on the public sector side, so I'll speak more to that.

There needs to be clear establishment of no-go zones, again, for example, in terms of mass surveillance of public places. There need to be clear rules around the issuance of privacy impact assessments.

We believe it would be powerful to have mandatory third party and independent review of algorithmic and biometric surveillance tools used by law enforcement so that they would be assessed for their human rights impact as well as for their accuracy and concerns around bias.

We believe one thing that could also help is that there would be a government agency specifically for following, studying and creating a repository and directory of the use by federal agencies of algorithmic and biometric tools in general, but especially in regard to surveillance.

● (1635)

Mr. Ryan Williams: Thank you, sir.

The Chair: Now we'll go to Mr. Bains for five minutes.

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

My questions are coming from Richmond, British Columbia. I'm concerned about this and the use of AI. As you know, in British Columbia, we have a strong BIPOC community, predominantly Asian and South Asian. We also heard from a witness the other day about a flag that the VPD is using AI.

My question is directed to Dr. McPhail. Vancouver Police Chief Adam Palmer assured the police board in April 2021 that his officers will not use facial recognition technology for investigations until a policy is in place.

Do you know if any FRT policy has been put forward to the police services board?

Ms. Brenda McPhail: I do not know, in the context of Vancouver, whether such a policy has been put forward.

I do know that in Toronto what we believe to be the first such policy was recently put through, and the grapevine has suggested that many other police forces across Canada were waiting on that to happen in order to take a look at it and to construct their own policies accordingly. However, I apologize; I don't know specifically about the state of that policy in Vancouver.

Mr. Parm Bains: Have you been apprised of that flag the previous witness may have indicated, which is that AI is already being used?

Ms. Brenda McPhail: Yes, I believe that came from the extensive research conducted in the Citizen Lab report on algorithmic policing across Canada.

There are a number of forces across Canada, including Vancouver's, that are currently engaged in using these kinds of tools. It's happening quietly, under the radar, generally without any public revelations at the point of procurement, at the point of policy development or at the point of implementation. We have a real crisis of accountability when it comes to police use of these technologies.

Mr. Parm Bains: It's without a policy in place. Is that correct?

Ms. Brenda McPhail: Either there is no policy in place or there's not a policy that's available for public view. I've done extensive access to information requests on similar topics, most specifically focused on facial recognition technology, and it's like pulling teeth to get access to this information in any sort of reasonable way.

Mr. Parm Bains: In December of 2021, the CCLA supported the decisions of the B.C., Alberta and Quebec commissioners, which included binding orders to Clearview AI to cease collecting personal information in those provinces and to delete all personal information already collected without consent. Are you aware of any action that Clearview AI has taken on those orders?

Ms. Brenda McPhail: Indeed, Clearview AI has filed legal applications, lawsuits, against the commissioners in B.C., Alberta, Quebec and federally disputing those orders and challenging them on a series of grounds that range from the difficulty or impossibility of complying with those orders to challenging the constitutionality of Canada's privacy laws and arguing that they have a free expression right to data scraped from the Internet.

This is going to be ongoing litigation, and it's very worth the committee's attention.

● (1640)

Mr. Parm Bains: Thank you.

If I have time, I'd like to switch to Dr. LaPlante.

In January 2021 you co-authored an article in RBC Capital Markets, “Ensuring AI Remains a Force for Good”. You talk about the Respect AI program as a way to build public trust. One of the ways you indicate this can be done is by using technology to expose bias.

Back to my colleague Mr. Fergus's question about the technology that's capturing the images, can you provide the committee with some ideas or examples on how technology can be used to root out these inherent biases?

The Chair: Please give a very brief answer.

Dr. Alex LaPlante: I think that's going to be a very difficult one to answer quickly, but one thing I will maybe suggest that you look into is this concept of ethics by design, which is essentially taking ethical considerations throughout your development cycle from initial data collection through algorithmic development and through questions you should ask yourself around productionization and the monitoring of those systems. There's a lot of detail you can pull together on that. There are a number of organizations that practise in that, as does Borealis.

The Chair: Mr. Bains and Ms. Saks, I called you in the wrong order from what I was provided. I wrote you down out of order, so I apologize. If I should ever, at the committee, call speakers who aren't expecting to be called, just give me a quick correction, and we'll get the person who should be called.

[*Translation*]

On that note, I'll give the floor to Mr. Garon for two and a half minutes.

Mr. Jean-Denis Garon: Thank you, Mr. Chair.

I'll continue with Mr. Labonté.

I'd like to get back to the question from my colleague Mr. Fergus. Earlier, he asked if it was necessary to start over from scratch, and take the time required to come up with appropriate regulations. But then companies like Clearview AI have already gathered and stored a staggering number of photographs.

Have we already waited too long to establish a regulatory framework?

Mr. Françoys Labonté: It's too late to regulate data harvesting, because we can't go back in time. However, we can regulate the use of technology.

What people don't always understand very clearly is that the idea driving the technologies we are talking about is acquiring lots of data and using it to train the systems. The desired outcome is facial recognition, meaning the ability to identify whether someone is such and such a person. It creates an explicit model. In technology and engineering, there is usually a data entry phase during which information is processed with a view to results. That's not the model here. Now, implicit models are created which, on the basis of observation, processing and the analysis of many data sets, can provide the expected results. The players who succeeded in doing that by collecting all kinds of data over the past 10 years now have a competitive advantage compared to these models. It's something that's very difficult to reproduce. They are true black boxes.

My view is that this would be extremely difficult, because you can't travel back in time.

Mr. Jean-Denis Garon: I have only 30 seconds left, so I'll ask you a brief question.

Given the quantity of data out there, is regulating its use like regulating tax evasion, in the sense that countries would have to coordinate with one another to provide a proper framework?

Mr. Françoys Labonté: That would very likely be necessary.

The crux of the matter is the stockpile of data. A glance at the numbers that show how the situation has evolved show that the quantity of data being stored in cloud platforms is exponential. Once the wheel starts to turn, it's difficult to turn it back.

● (1645)

[*English*]

The Chair: Thank you, Monsieur Labonté.

We have Mr. Green for two and a half minutes.

Mr. Matthew Green: Thank you.

I'll start my line of questioning with Dr. LaPlante. In her testimony, I believe she spoke about the need for private sector accountability. I wonder if she would contemplate and share any legislative frameworks that would provide true accountability should third party corporations use this in bad faith or in ways that are egregious violations of privacy.

Dr. Alex LaPlante: I'll focus my comments on AI regulation broadly. Right now in Canada, we lack an end-to-end regulation, and there are several changes that need to be made. I'll point you in the direction of a recent framework published by the EU Commission—this is a draft framework, but it's very likely to go into practice in 2022—that tackles issues of artificial intelligence and the risks associated, anything from privacy and human rights to very technical concepts of robustness and stability.

Ultimately, every time we develop one of these systems, we should be doing an impact assessment. As I noted in my remarks, the oversight of these systems should be based on risk materiality, meaning for very high-risk systems. There should be some level of scrutiny in the requirements around their usage and testing. Testing covers a very broad range of technical concepts, like robustness, stability, bias and fairness, and thresholds have to be put in place. Granted, these are context-dependent, so they would have to be put in place by the developers in order for us to ensure that there is accountability.

I will also note—and this is something I think is often forgotten—that these systems are stochastic. This means that when we put them in production, we may have a really good sense of how they'll behave today, but as our data changes in the future, we need to make sure we're continually monitoring the systems to ensure that they are working in the way we had initially intended. If they're not working in that way anymore, they need to be pulled from production and reassessed before they are put back out. This is particularly true in high-risk use cases like criminal identification.

Mr. Matthew Green: On that, my last question is to Ms. McPhail. From your perspective, where law enforcement has used this technology, do you know of any instances where there have been false positives that have caused material harm to the innocent people who were identified?

The Chair: Answer very briefly. Thank you.

Ms. Brenda McPhail: In Canada, in part because police forces have been cautious and measured in adopting this technology and are using it in relatively limited ways, I do not know of such examples.

In the United States, where the uptake has been faster and less cautious, our sister organization, the American Civil Liberties Union, currently has litigation in several states fighting for men—all of them Black—who were misidentified by this technology. One in particular, Mr. Williams, had police come to his home, handcuff him and drag him out of his home in front of his minor children.

The Chair: Thank you, Ms. McPhail.

We go now to Mr. Bezan.

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

I want to thank the witnesses. It has been very informative and eye-opening for all of us here, knowing what is at stake.

I'll just follow up on the questioning Mr. Green started off on.

With my background in national defence and security, I hadn't even thought about how facial recognition technology is being used to violate the charter rights, and even the Criminal Code and the National Defence Act, which say you can't spy on someone directly or indirectly unless warrants have been issued or, in case of an imminent threat, ministerial authorization was given. There are checks and balances through that whole process.

When we start looking at the mass collection and mass surveillance using FRT, how do we even say it's possible when we know that there are supposed to be all these checks and balances under the Criminal Code, the charter and the National Defence Act as it applies to CSE? You think about CSIS and the Canada Border Services Agency, never mind the RCMP, OPP and all the other policing organizations that are out there.

I would be interested on a quick take from Mr. McSorley and Ms. McPhail on that.

Mr. Tim McSorley: While it's true that there are rules in place to minimize mass surveillance from those agencies, as was mentioned, in recent draft guidance to law enforcement agencies, the Privacy Commissioner raised the concern that because the laws around this are currently a patchwork, there are concerns that there are loopholes and that there will be ways for federal agencies and law enforcement agencies to engage in mass surveillance that otherwise would be considered unlawful.

There's a lack of clarity around that right now. The lack of discussion and the lack of forthcomingness from federal agencies to discuss their use of facial recognition technology is what raises these deep concerns that they could be engaging in forms of surveillance that are unlawful or which otherwise would be considered unlawful, but are doing so because of this patchwork of legislation.

There are also debates around what's considered mass surveillance. For example, the RCMP scrape information about individuals online and keep those in databases. We know they have been doing that. This is beyond facial recognition, but they would argue they have a right to collect that information, whereas others have been challenging it as we have, saying that it's a form of mass surveillance that needs to be regulated.

● (1650)

Mr. James Bezan: You're saying then, Mr. McSorley—I'll let Ms. McPhail jump in on this as well—that the scraping of images off social media of people who participate in mass protests like we recently had here in Canada, as well as mass surveillance and FRT, would be violations of their civil liberties, in your both opinions?

Ms. McPhail.

Ms. Brenda McPhail: Mr. Chair, yes, I believe so.

In our current legislative regime, there are wide gaps that seem to have been exploited at this time to allow some uses of this technology in ways that have yet to be critiqued or examined in front of a judge. I think that's going to happen probably in the near future here in Canada, but it can be pre-empted if we sit down and think very carefully through whether there are ways this can be done safely.

In some cases, the answer is going to be no. CCLA supports a complete ban on mass surveillance uses of this technology.

In some cases, such as the current police use of facial recognition technology in conjunction with mug shot databases, for example, even those uses are not necessarily uncontroversial. We simply haven't thought about them. Police use of FRT for mug shot databases is being conducted on legacy databases that have their own issues of bias and discrimination that we have known about for a really long time.

I think it's not just the mass surveillance aspects of this, but also the more targeted ones that we haven't grappled with.

Mr. James Bezan: If we get talking about targeted ones, we have with us Ms. LaPlante from Borealis AI, which is working with RBC. We know that the RCMP and the government wanted to freeze the bank accounts of people who participated in the recent protest.

How do we start...?

Would some of the technology that Borealis AI has be used in allowing the government to freeze the bank accounts of certain individuals whose faces were scraped from social media or mass surveillance through other means, such as drones and cameras?

The Chair: I would ask for a brief response. Mr. Bezan used all his time asking, so give a very brief response.

Dr. Alex LaPlante: It's a resounding no.

As I mentioned, we take ethics very seriously in the design of any of our algorithmic systems. This was definitely not a use case that would have come across our desk at RBC.

The Chair: Thank you for that.

Ms. Saks, go ahead for five minutes.

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

Thank you to all of our witnesses today.

Through you, Mr. Chair, I'd like to start off my questions with Ms. McPhail.

Obviously, we're dealing with massive amounts of data and a massive proliferation of the use of FRT and AI. As Mr. Labonté mentioned earlier, there are grey zones in its use in the retail sector. Other witnesses talked about health care and other beneficial uses, and we know there is that debate back and forth.

In the request for a moratorium, my question to you is where we start.

There are gaps in the legislation right now that don't target the private sector, and they're the ones manufacturing this technology, so who exactly are we putting a moratorium on?

● (1655)

Ms. Brenda McPhail: CCLA particularly supports a moratorium for police and national security uses of this technology, because those are situations where the consequences, if we get them wrong, are literally life-altering for individuals.

That said, it would be beneficial to have a general moratorium, because what we know is that private sector vendors are selling technologies to public sector actors, including law enforcement and national security bodies. The way that our current privacy law regime works is that those two sides, public and private, are governed in some ways under different sets of regulations, which only exacerbates the difficulty of effectively regulating this area.

We really need a coherent approach to thinking through how to develop protections in this regard.

Ms. Ya'ara Saks: I appreciate that. I'd like to dig into that a little deeper, because the truth of the matter is that if we ask the question.... As a kid, my dad used to tell me all the time to ask the question *quanto uno*: who benefits?

With private sector companies offering this technology to security surveillance, whether it's the police forces or the RCMP, we've entered this grey zone. In your recommendations to the Privacy Commissioner, have you addressed that grey zone of those loopholes in implementing a more...?

The question is, if you're asking for a moratorium, how do we make sure one works? It's so widespread at this point that to make it effective.... I'm asking what the efficacy would be.

Ms. Brenda McPhail: It's a good question. One of the major gaps in our privacy regime is that our federal commissioner does not have enforcement powers and cannot issue binding orders. One purpose of a moratorium would be to give the government a chance to rectify that gap, should it choose to do so.

There's always the question when you make a law of whether people will follow it. If you issue an order, will people comply? I think we're all very aware of the risks of that kind of equation after living through all these years of this pandemic. The fact that it may or may not be 100% effective in every regard doesn't mean that it's not necessary and it doesn't mean that we shouldn't try, because the stakes are so high. We are talking about the charter-protected rights of people across Canada who are at risk every day we allow these technologies to continue to be used without the legal safeguards in place to protect them.

Ms. Ya'ara Saks: My question now is to Mr. Labonté. We know that a lot of the AI technology that is out there has issues in discriminating against non-whites. Steve Lohr from The New York Times said at one point—I think it's a low number, actually—there's a 35% inaccuracy when it comes to discriminating against non-whites, women and children. I assume it might be higher than that, especially in light of the 2019 NIST report.

Who is designing this technology? Are we asking those questions and making sure that these algorithms and the design of this technology have a visible minority and racialized lens from where you sit at CRI?

Mr. Françoys Labonté: We don't have a lot of time, but if we go back many years to when we were doing statistics, normally we were designing experiments to make sure that our samples were representative so that at the end we would get statistically significant results.

Now we're in a world where there is just a lot of data, and you take whatever you have, and it gives what it gives.

The issue of designing systems based on the representativeness of data is a key issue. Very often, when we say that systems are biased, it's just that the initial data samples are not equal or are not representative in an equal way. This is the challenge generally. It's not the technology per se; it's the data that has been provided to the system.

Dr. LaPlante mentioned all the issues with AI. It points to something like our AI system becoming a critical system that should be regulated. It's like when you design cars or airplanes; you have to demonstrate all these issues of reliability, reproducibility and all these elements. A lot of these questions point to this, in fact.

AI is still the new generation—

● (1700)

The Chair: I'm really sorry to interrupt, but that went substantially over time, and I am going to have to conclude that round.

We've completed the first two rounds. We have half an hour to go. We expect bells to ring in probably about 15 minutes, but we'll carry on with more questions.

We will go to Mr. Kurek, for five minutes, followed by Ms. Kayabaga.

Mr. Damien Kurek: Thank you very much, Mr. Chair.

First, let me take this opportunity to thank all of the witnesses, as it's been a very enlightening and I think meaningful conversation. I think all parties would agree that the subject and real substance of what we're getting to here is very valuable for our country.

Mr. Chair, if you would indulge me, I would use these few moments of my time to move the motion that I gave verbal notice of on March 3 of this year. I'll read that into the record once again:

> That, pursuant to Standing Order 108(3)(h), the committee undertake a study into issues of conflict of interest and the Lobbying Act in relation to pandemic spending, provided that: (a) the evidence and documentation received by the committee during both sessions of the 43rd Parliament on the subject be taken into consideration by the committee in the current session; (b) the committee adopt the report entitled Questions of Conflict of Interest and Lobbying in Relation to Pandemic Spending, originally adopted as the committee's second report in the second session of the 43rd Parliament; (c) dissenting or supplementary opinions be submitted electronically in both official languages to the clerk of the committee within 48 hours of the adoption of this motion; (d) the chair table this report in the House on or before March 31, 2022.

Mr. Chair, I will keep this very brief, as I hope we will find support among members of the committee to simply do this, not reopen this issue but rather to acknowledge the hard work that was done by members of this committee prior to the election that was called last summer, and to ensure that Canadians have a chance to see the report that all members of this committee worked on. I believe there are members from most parties who are still sitting on this committee from the last Parliament.

With that, Mr. Chair, I would move this motion.

The Chair: All right, Mr. Kurek, you have moved the motion.

Are you going to speak further on the motion, because I have other speakers? If you're done, then I am going to go to debate on the motion.

Mr. Damien Kurek: Mr. Chair, I would simply say that I have endeavoured to be as uncontroversial as possible. I would leave it at that.

The Chair: Thank you.

The motion is moved. It was on notice, and given the date there, it's not surprising today that we're going to have to deal with it.

I have Mr. Fergus first. I'll put you on the order. I have several.

Go ahead, Mr. Fergus.

[*Translation*]

Hon. Greg Fergus: I'm dumbfounded.

[*English*]

I'm surprised that, during a particularly important discussion we're having on facial recognition, where all parties seem to be expressing some grave concerns on this technology and how it affects especially people of colour, women and young people, we would play this game, and it is a bit of a game.

Mr. Chair, contrary to what my respected colleague had indicated, as far as I can see, I'm the only one who was on the committee from last year when we went through this very long debate, and then we went through, I think, a very substantive report.

May I add, Mr. Chair, for the members, for every other member who was not on the committee at the time, that every recommendation sought by the party of the member opposite was adopted in that report, every single one? It was presented to the House. I am trying to figure out why, almost one year later, we're going back through this again.

We've done some really good work in this Parliament. I sit on this committee. I sit on PROC. I've been impressed by the goodwill of members to try to put down their narrow partisan interest for the benefit of Canadians and get to some really good initiatives.

This discussion on facial recognition has been sitting around for not one year, not two years, but three years. Three years have gone by when we could have acted on this. More scraping of faces from the Internet and more people facing unfair targeting by using this technology have happened over three years. Now we're going to open up something that we have spent countless hours debating, not only debating but coming up with a report on. My friend's party got every single recommendation it sought, unamended. Are we going to go back into this again? That's a waste. It's a disappointment. I have to say, frankly, that it makes me very angry.

We've been trying to get at this study for three years. We finally got here, and every question here today....

● (1705)

[*Translation*]

Hats off to all my friends here around the table for their serious questions.

So now we're going to play politics with something we settled a year ago, and which has already been presented to the House of Commons?

Mr. Chair, it's ridiculous and it's insulting. It's mind-boggling.

[*English*]

It's really deeply disappointing.

Thank you, Mr. Chair.

The Chair: Thank you, Mr. Fergus.

I have quite a speaking list now.

Next I have Ms. Khalid.

Ms. Iqra Khalid: Thank you very much, Mr. Chair.

I echo the sentiments of my colleague. I thank the witnesses today for appearing and helping our endeavour into this really important legislation.

As Mr. Kurek was reading the words of his motion, I actually had a copy of a motion on December 13 that had been moved by Mr. Brassard in this very committee. It was word for word the exact same motion.

I know that in our *House of Commons Procedure and Practice*, chapter 20, under "Format and Admissibility" of motions, it says:

> A motion that is the same in substance as one already decided in the same session is inadmissible; however, a member may move a motion which, although similar, is sufficiently different as to constitute a new question.

I do see that the only difference between Mr. Kurek's motion as he's presented today and the previous one from Mr. Brassard is that there's a new section, (d), which just adds a timeline to the exact same substance.

Can I humbly request your ruling on this as to whether this motion is actually in order or not?

● (1710)

The Chair: I accepted this motion when it was made. It does contain a couple of differences and I have ruled it in order. That is my ruling.

Ms. Iqra Khalid: Mr. Chair, in that case, having listened to the words from Mr. Kurek and having compared them to the exact same motion that was voted on and defeated in this committee on December 13, I would appeal your decision.

The Chair: Ms. Khalid has challenged my ruling that this motion is in order. I'll ask the clerk to commence the vote.

Mr. James Bezan: To be clear, it's that the ruling of the chair stands, right?

The Clerk: Exactly. I will actually explain that.

There was debate on a motion, the chair ruled the motion admissible, and Ms. Khalid is challenging the decision of the chair.

The question is whether the decision of the chair on the motion from Mr. Kurek be sustained.

If you think the decision of the chair that the motion is admissible is correct, you vote yes.

If you think the decision of the chair is incorrect and that the motion should be considered inadmissible, you vote no.

(Ruling of the chair sustained: yeas 6; nays 5)

The Chair: Ms. Khalid, you had the floor and you still have the floor if you have anything to add. Otherwise, I will go to the next speaker.

Ms. Iqra Khalid: Yes, Mr. Chair.

In that case, I will start by apologizing to our witnesses today for their cut time in the important testimony they had to provide for us today on this very important work that we are doing.

I would ask, through you, Mr. Chair, that if there any additional items that they would like to have highlighted based on the questioning and on what they've heard from each other and members today, then perhaps they could provide those in writing. We would greatly appreciate those submissions. We hope we can get back to this study in a reasonably quick fashion.

I will also say, Mr. Chair, that I am quite disappointed. As I said, these are literally, word for word, the exact same words that on December 13 were already voted on and defeated. We went on to study a lot more important things, as Mr. Fergus very clearly outlined. We are now back to square one. We will now be spending a lot of time, I think, debating the merits of a motion that we had already spent a lot of time debating the merits of.

I would hope that the committee would understand the importance of why we need to move on to this facial recognition study. We are a country that really needs to have strengthened privacy laws and laws around the regulation of industry taking advantage of the privacy of Canadians. We really need to reform PIPEDA. It was put in place a long time before facial recognition and artificial intelligence came into the picture.

I am hoping we'll get back to that and to studying more relevant issues that we haven't already rehashed. As Mr. Fergus said, we have been waiting to start this study for the past three years. I can't begin to really highlight how important it is that we continue to move forward with this study and that we put forward some serious, strong recommendations for reforming how industry and how technologies like artificial intelligence and facial recognition need to be curbed to make sure that we strike that balance. One of our witnesses, I believe it was Mr. Labonté, talked about the balance between privacy, social acceptance and societal benefits—

● (1715)

Mr. James Bezan: I have a point of order.

The Chair: There has been a point of order.

Mr. Bezan, state your point that is—

Mr. James Bezan: The point of order is relevance. Ms. Khalid's comments have nothing to do with the motion. She's talking about the study that we were talking about earlier. We should be getting back to business.

We have a lot of time here. We could get back to the study if we just had the vote.

The Chair: Thank you, Mr. Bezan.

I was allowing Ms. Khalid some latitude in her remarks that were straying a little bit outside the motion itself.

It has come to my attention that bells are ringing. At this point, I will require the unanimous consent of the committee to continue.

I see heads shaking.

With that, the meeting is adjourned.