HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

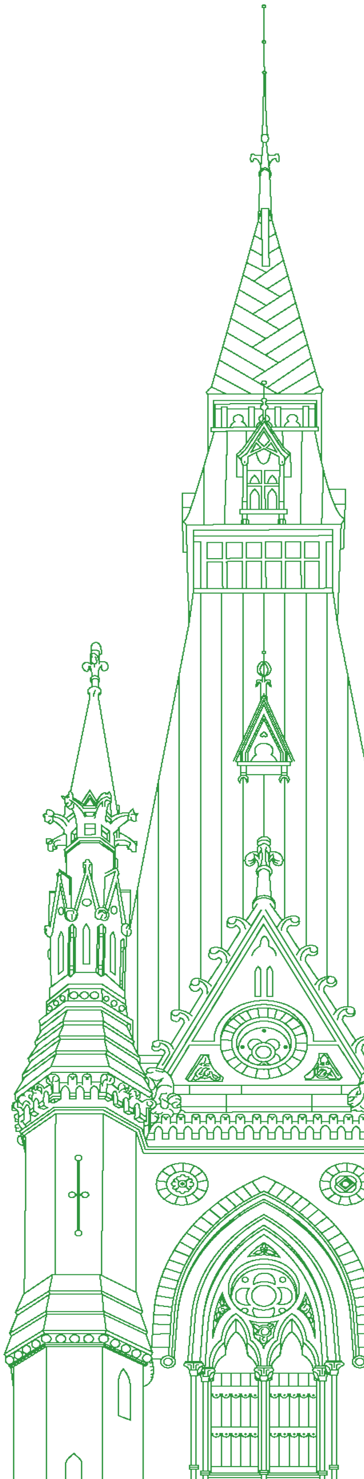
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 011

Monday, March 21, 2022



Chair: Mr. Pat Kelly

Standing Committee on Access to Information, Privacy and Ethics

Monday, March 21, 2022

● (1100)

[*English*]

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

Welcome to meeting number 11 of the House of Commons Standing Committee on Access to Information, Privacy and Ethics.

[*Translation*]

Pursuant to Standing Order 108(3)(h) and the motion adopted by the committee on Monday, December 13, 2021, the committee is commencing its study of the use and impact of facial recognition technology.

[*English*]

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. As 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 you've heard them many times now and I won't repeat them all, but I encourage everyone to follow them.

I would also remind all participants that no screenshots or photos of your screen are permitted. When speaking, please speak slowly and clearly for the benefit of translation. When you are not speaking, your microphone should be on mute.

Finally, I will remind all of you that comments by members and witnesses should be addressed through the chair.

I now welcome our witnesses for the first panel. We have, as an individual, Ms. Cynthia Khoo, who is a research fellow at the Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto.

From INQ Law, we have Ms. Carole Piovesan, who is a managing partner.

We'll begin with Ms. Khoo. You have up to five minutes for your opening statement.

Ms. Cynthia Khoo (Research Fellow, Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto, As an Individual): Thank you, and good morning.

My name is Cynthia Khoo and I am an associate at the Center on Privacy and Technology at Georgetown Law in Washington, D.C., as well as a research fellow with the Citizen Lab at the University of Toronto.

I am here today in a professional capacity, though I am providing my own views as an individual based on my work at the Citizen Lab and which are further informed by the work of my colleagues at both the Citizen Lab and the Privacy Center.

Today I'll discuss four key concerns with police use of facial recognition technology, each with a proposed recommendation.

To begin, I'll introduce you to three people: Robert Williams was singing in his car when a crime he had nothing to do with occurred; Nijeer Parks was transferring funds at a Western Union; and Michael Oliver was simply at work.

All three are Black men who were wrongfully arrested by police relying on facial recognition technology. They have endured lost jobs, traumatized children and broken relationships, not to mention the blow to personal dignity. These are the human costs of false confidence in, and unconstitutional uses of, facial recognition technology.

This is the same technology that researchers have found is up to 100 times more likely to misidentify Black and Asian individuals, and that misidentifies more than one in three darker-skinned women, but does work 99% of the time for white men.

Although I used examples from the United States, the same could easily happen here, if it hasn't already. Racial discrimination against Black and indigenous people imbues every stage of the Canadian criminal justice system, from carding, arrests and bail to pleas, sentencing and parole. Embedding facial recognition algorithms into this foundation of systemic bias may digitally alchemize past injustices into an even more and perhaps permanently inequitable future.

Therefore, recommendation number one is to launch a judicial inquiry into law enforcement use of pre-existing mass police datasets, such as mug shots. This is to assess the appropriateness of repurposing previously collected personal data for use with facial recognition and other algorithmic policing technologies.

I turn now to my second point. Even if all bias were removed from facial recognition, the technology would still pose an equal or even greater threat to our constitutional and human rights. Facial recognition used to identify people in public violates privacy preserved through anonymity in daily life and relies on collecting particularly sensitive biometric data. This would likely induce chilling effects on freedom of expression such as public protests about injustice. Such capability also promises to exacerbate gender-based violence and abuse by facilitating the stalking of women who are just going about their lives and who must be able to do so free of fear.

Facial recognition has not been shown to be sufficiently necessary, proportionate or reliable to outweigh these far-reaching repercussions. Thus, recommendation number two is to place a national moratorium on the use of facial recognition technology by law enforcement until and unless it's shown to be not only reliable but also necessary and proportionate to legitimate aims. This may well mean a complete ban in some cases, as several U.S. cities have already done. Canada should not shy away from following suit. This software cannot bear the legal and moral responsibility that humans might otherwise abdicate to it over vulnerable people's lives and freedom.

The third problem is lack of transparency and accountability. That this is a problem is evident in that the public knows about police facial recognition primarily only through media, leaked documents and FOI requests. Policies governing police use of facial recognition can be even more of a black box than the algorithms themselves are said to be. This circumstance gives rise to severe due process deficits in criminal cases.

Recommendation number three is to establish robust transparency and accountability measures in the event such technology is adopted. These include immediate and advance public notice and public comment, algorithmic impact assessments, consultation with historically marginalized groups and independent oversight mechanisms such as judicial authorization.

Fourth and last, we need strict legal safeguards to ensure that police reliance on private sector companies does not create an end run around our constitutional rights to liberty and to protection from unreasonable search and seizure. Software from companies such as Clearview AI, Amazon Rekognition and NEC Corporation is typically proprietary, concealed by trade secret laws and procured on the basis of behind-the-scenes lobbying. This circumstance results in secretive public-private surveillance partnerships that strip criminal defendants of their due process rights and subject all of us to inscrutable layers of mass surveillance.

I thus conclude with recommendation number four. If a commercial technology vendor is collecting personal data for and sharing it with law enforcement, they must be contractually bound or otherwise held to public interest standards of privacy protection and disclosure. Otherwise the law will be permitting police agencies to do indirectly what the Constitution bars them from doing directly.

Thank you. I welcome your questions.

● (1105)

The Chair: Thank you.

Now, for five minutes, we have Ms. Piovesan.

Ms. Carole Piovesan (Managing Partner, INQ Law): Thank you, Mr. Chair and members of the committee. Good morning.

My name's Carole Piovesan. I'm a managing partner at INQ Law, where my practice concentrates in part on privacy and AI risk management. I'm an adjunct professor at the University of Toronto's Faculty of Law, where I teach on AI regulation. I also recently coedited a book on AI law, published by Thomson Reuters in 2021. Thank you for the opportunity to make a submission this morning.

Facial recognition technologies, FRTs, are becoming much more extensively used by public and private sectors alike, as you heard Ms. Khoo testify. According to a 2020 study published by Grand View Research, the global market size of FRTs is expected to reach $12 billion U.S. by 2028, up from a global market size of approximately $3.6 billion U.S. in 2020. This demonstrates considerable investments and advancements in the use of FRTs around the world, indicating a rich competitive environment.

While discussions about FRTs tend to focus on security and surveillance, various other sectors are using this technology, including retail and e-commerce, telecom and IT, and health care. FRTs present a growing economic opportunity for developers and users of such systems. Put simply, FRTs are becoming more popular. This is why it is essential to understand the profound implications of FRTs in our free and democratic society, as this committee is doing.

For context, FRTs use highly sensitive biometric facial data to identify and verify an individual. This is an automated process that can happen at scale. It triggers the need for thoughtful and informed legal and policy safeguards to maximize the benefits of FRTs, while minimizing and managing any potential harms.

FRTs raise concerns about accuracy and bias in system outputs, unlawful and indiscriminate surveillance, black box technology that's inaccessible to lawmakers, and ultimately, a chilling effect on freedom. When described in this context, FRTs put at risk Canada's fundamental values as enshrined in our Canadian charter and expressed in our national folklore.

While the use of highly sensitive, identifiable data can deeply harm an individual's reputation or even threaten their liberty—as you heard Ms. Khoo testify—it can also facilitate quick and secure payment at checkout, or help save a patient's life.

FRTs need to be regulated with a scalpel, not an axe.

The remainder of my submission this morning proposes specific questions organized in four main principles that align with responsible AI principles we see around the world, and are intended to guide targeted regulation of FRTs. The principles I propose align with the OECD artificial intelligence principles and leading international guidance on responsible AI, and address technical, legal, policy and ethical issues to shape a relatively comprehensive framework for FRTs. They are not intended to be exhaustive, but to highlight operational issues that will lead to deeper exploration.

The first is technical robustness. Questions that should inform regulation include the following. What specific technical criteria ought to be associated with FRT use cases, if any? Should there be independent third parties engaged as oversight to assess FRT from a technical perspective? If so, who should that oversight be?

Next is accountability. Questions that should inform regulation include the following. What administrative controls should be required to promote appropriate accountability of FRTs? How are those controls determined and by whom? Should there be an impact assessment required? If so, what should it look like? When is stakeholder engagement required and what should that process look like?

Next, is lawfulness. Questions that should guide regulation include the following. What oversight is needed to promote alignment of FRT uses with societal values, thinking through criminal, civil and constitutional human rights? Are there no-go zones?

Certainly last, but not least, is fairness. Questions associated with fairness regulation include the following. What are the possible adverse effects of FRTs on individual rights and freedoms? Can those effects be minimized? What steps can or should be taken to ensure that certain groups are not disproportionately harmed, even in low-risk cases?

● (1110)

Taken together, these questions allow Canada to align with emerging regulation on artificial intelligence around the world, with a specific focus on FRTs given the serious threat to our values as balanced against some of the real beneficial possibilities.

I look forward to your questions. Thank you.

The Chair: Thank you very much.

We'll go to the first round of questions.

First up is Mr. Williams for six minutes, please.

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

Thank you very much to our panellists this morning for coming on board.

I'll start with you, Ms. Khoo. I'd like to clarify a question I had from your recommendations. You have recommended a moratorium on facial recognition technology at this point. Is that correct?

Ms. Cynthia Khoo: It's a moratorium on the use of facial recognition technology by law enforcement. The reason it's a moratorium and not a ban is that essentially the moratorium would give time to look further into the issue—to launch a judicial inquiry, for example—until we can determine whether it is appropriate to use facial recognition, under what circumstances and with what safeguards, and then include the time to put those safeguards in place.

Mr. Ryan Williams: Thank you.

In September of 2020, you wrote the following:

> The Canadian legal system currently lacks sufficiently clear and robust safeguards to ensure that use of algorithmic surveillance methods—if any—occurs within constitutional boundaries and is subject to necessary regulatory, judicial, and legislative oversight mechanisms.

I think it falls within that theme. We know that right now algorithmic surveillance methods are still here. Could you tell the committee what kind of safeguards we need in order to properly protect Canadian rights today?

Ms. Cynthia Khoo: Absolutely. I would say that the first one off the bat is transparency. A lot of the knowledge we have of what is even in place these days, as I mentioned, comes because of investigative journalists or document leaks, for example, when it ideally should be law enforcement and the government telling us that up front, ideally prior to adoption, and giving the public a chance to comment on the potential impacts of these technologies. That's the first thing.

The second thing is that we need oversight mechanisms that will assess—either of the impact assessments, for example—ahead of time and not after the fact the potential harms of these technologies, particularly with respect to historically marginalized communities.

These are kind of higher-level principle safeguards, but going more into the weeds, our report focused on the criminal law context. Another example of safeguards would be that in the case of specific criminal defendants, there should be disclosure requirements so that it's known if these types of technologies have been used in their case, for example, and they have an opportunity to respond.

● (1115)

Mr. Ryan Williams: Thank you.

In this committee's other ongoing study about the collection and use of mobility data, we heard about the absence of prior and informed consent on the use of personal data and information. How important is it for any collection of Canadians' personal information to have clear and informed consent prior to the collection being undertaken?

Ms. Cynthia Khoo: I would say as a starting principle that it is extremely important that all residents of Canada are able to give prior and informed consent to their data being collected. I understand that this is complicated in the criminal justice context, but I think this is where the connection to commercial vendors becomes really salient. Commercial vendors are collecting so much data that should be done under prior and informed consent, but it is not. In some cases, it is either permitted to not be or it is just not in practice. That data gets funnelled through to law enforcement agencies. On this issue, I think that's something that warrants a lot of attention from this committee.

Mr. Ryan Williams: Thank you.

Ms. Piovesan, are there any current protections in Canadian law for the uses of collected facial recognition data? To clarify, I mean protection regarding how, where and for how long it's stored, and how it can be used or sold.

Ms. Carole Piovesan: There are some protections under privacy law that we look at. Again, it depends on who is conducting the collection. If we're talking about a state actor, there is a patchwork of regulation and common law that will govern how certain information can be collected, stored, retained. Under federal private sector privacy law, for instance PIPEDA, there are certainly requirements that would, as Ms. Khoo said, demand that companies that want to collect such sensitive data do so on the basis of consent. If you look at Quebec, for instance, given that facial recognition technology involves biometric data, you'd be looking at a consent requirement as well. We do have a patchwork, depending on who the actor is who's actually leading that collection.

The issue is that we don't have comprehensive regulation, or frankly, a comprehensive approach when it comes to the use of facial recognition technology as a technology from soup to nuts, meaning that from the collection of that data through to the actual design of the system through to the use of that system, having a clear understanding of the appropriate safeguards in place from beginning to end, including that collection and storage of that data, the assessment of that data, the disclosure requirements around that data. Whether it's a public or non-public actor, there are different disclosure requirements, potentially, but disclosure requirements nonetheless. We have a right to know when aspects of our faces or anything that's an immutable, sensitive data point is being collected and stored and potentially used in a way that could be harmful against us.

Really, again, we have this patchwork of laws and regulations, depending on who the actor collecting that information is, but we don't have a comprehensive or really focused law around facial recognition technology.

Mr. Ryan Williams: Okay. Thank you very much.

The Chair: We'll go next to Mr. Fergus for six minutes.

[*Translation*]

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

I'd like to thank our two witnesses for their presentations.

I rarely do this, but today I'm going to speak in English.

[*English*]

This is an issue on which I've done most of my reading in English, so I'll continue asking my questions in English.

First of all, let me thank Ms. Piovesan as well as Ms. Khoo for their contributions, not only to our study here but in terms of what they've written and published beforehand.

Ms. Khoo, I'd like to start with you. I've read a number of articles you've been involved with. One that certainly has caught my attention is one you co-authored in the Citizen Lab report. For the purposes of this committee I think it would be really important if you were to briefly explain what algorithmic technologies are. Then I'm going to have a few questions that are going to move on from there.

● (1120)

Ms. Cynthia Khoo: That is great question. Algorithmic technologies can be very broad, depending on what level you're defining them at. In our report we defined algorithmic policing technologies specifically. If you think about it, an Excel spreadsheet could potentially be an algorithmic technology, in the sense that it relies on algorithms.

Algorithmic policing technologies, for the purposes of scoping our report—and I suspect it would probably be helpful in scoping for your committee—are emerging technologies that rely on automated computational formulas that are often used to assist or supplement police decision-making.

Hon. Greg Fergus: When we take a look at these algorithmic technologies, they're based on data that is collected by police—and I think you make a very good argument here, but for the purposes of the committee again—which in itself has been shown to have a pretty strong bias in the collection of that data. Is that not correct?

Ms. Cynthia Khoo: That's correct.

Hon. Greg Fergus: Any algorithmic approach we would adopt in terms of collecting, using for artificial intelligence purposes, frankly, we would just be exacerbating these biases.

Ms. Cynthia Khoo: I think that would be true in a lot of cases, yes.

Hon. Greg Fergus: In that case, then, I very much understand your secondary recommendation for there to be a national moratorium on the use, by law enforcement, of these kinds of technologies. The question is—and I'm fascinated to find out—why do you limit it to that? Why wouldn't you want to put a moratorium on the scraping of this kind of information by the private sector or non-public sector organizations?

Ms. Cynthia Khoo: That is a really excellent question.

The reason I focused my remarks and will focus most of my comments today on the criminal justice context is purely because that was the scope of my research. I don't want to speak too far afield from issues that I've actually done that immersive study of myself, first-hand.

However, I do think there are a lot of really good reasons to engage in the same level of depth of research in the use of facial recognition not only in the commercial sector, but even by non-law enforcement government agencies. There may well be really good arguments to invoke a moratorium on facial recognition in those sectors as well. I can only speak more in depth to the policing context, but that's not to say that it wouldn't also be appropriate in these other contexts.

Hon. Greg Fergus: The reason I say this is that, as you pointed out, there is a possibility for people to do indirectly what they can't do directly while we work out the legal frame that could be used in terms of the establishment of the use of such technologies.

This technology really came to my attention three years ago now. One of the public broadcasters here in Canada, in Quebec, in French Canada, actually decided to use AI facial recognition technology to try to identify members of Quebec's National Assembly. As you say, and all studies have pointed out, if you are person of colour, if you are non-white, the error rate increases dramatically.

It would seem to me that it would behoove all of us to be careful in terms of trying to establish some limits as to how this information is collected and used in any context, not just in the criminal justice system.

Would you agree with that?

Ms. Cynthia Khoo: Yes, I think I would agree with that. Particularly, we've seen so many examples of emerging technologies, both facial recognition and other types of algorithmic policing technologies, where we as a society and human rights would really have benefited from a precautionary approach and not the infamous “move fast and break things” approach.

I do agree, though, with Ms. Piovesan, who talked about taking a more granular approach, a scalpel rather than an axe, but you're right. We do need time to figure out specifically what the contents of that approach are.

If being cautious and preventing harm means putting a stop to the use of this technology while we figure it out, it would be fair to say that's a sound approach.

Hon. Greg Fergus: I have only about 20 seconds left. Hopefully, I can borrow five seconds from my colleague.

Very quickly, is there anywhere in the world that has established a framework for the use of AI facial recognition?

● (1125)

Ms. Cynthia Khoo: I know that the European Union has been doing a lot of work in this area. They would be one jurisdiction, to start.

Also, the U.S. cities that I mentioned, particularly in California and Massachusetts, have been engaging in bans, moratoria and various frameworks of regulations to different degrees of strictness. That would be a potential model to look to as well.

Hon. Greg Fergus: Thank you very much.

The Chair: Thank you. That was very well timed.

With that, we will go to Mr. Villemure.

[*Translation*]

You have six minutes.

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

I want to thank the witnesses for their fantastic presentations.

I'm going to ask both witnesses the same question. I'd like very brief answers because I'll move on to something else after.

Ms. Khoo, does facial recognition mean the end of freedom?

[*English*]

Ms. Cynthia Khoo: Without more context around that statement, it might be somewhat broad to say facial recognition technology inherently means the end of freedom.

[*Translation*]

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

Ms. Piovesan, what do you think?

[*English*]

Ms. Carole Piovesan: I would agree with that. There are opportunities to use facial recognition technology that could be very beneficial. I gave the example of health care. Doing so and just having regular complete acceptance or denial of facial recognition, I don't think is the way to go. There are positive benefits, but there are some serious implications of the use of facial recognition technology, both of which have to be considered as we look to regulation.

[*Translation*]

Mr. René Villemure: Thank you very much.

I'll come back to you, Ms. Khoo. The number of images captured so far is almost impossible to assess. Does this mean that it's already too late to do something?

[*English*]

Ms. Cynthia Khoo: In terms of filling in some details, I imagine you might be talking about the three billion images captured by Clearview AI. In some respects, you could say it's too late in the sense that Clearview AI is already out there, they've already set up shop, they've sold contracts to all these police agencies, and even if they are no longer in Canada, they're still working in other countries. From that perspective, maybe it's too late.

However, it's never too late to act. For example, Clearview AI was operational in Canada at one point, and now they're not, because we found out and the OPC stepped in. There was public outcry. When it comes to technological issues, it's really easy to fall into a trap of technological inevitability or assuming that technology is here to stay. That is really not always the case.

Even when we talk about other types of algorithmic technologies, for example, the Federal Trade Commission in the United States has started issuing as part of their remedies in certain cases the disgorgement of algorithms: not only deleting data that has been illicitly collected, but even deleting the algorithmic models that have been built on top of that illicitly collected data.

[*Translation*]

Mr. René Villemure: Thank you very much.

Ms. Piovesan, is it too late?

[*English*]

Ms. Carole Piovesan: No. I agree with Ms. Khoo entirely.

We have seen some movements, particularly out of the FTC, to demand there be a disgorgement of the algorithm and a deletion of the data. We've increasingly seen movement to better regulate those entities that are using facial recognition technologies or broader artificial intelligence technology to demonstrate conformity with technical, administrative and other requirements, to show that they are appropriate for the market in which they will be used from a vendor perspective, and provide an impact assessment from the user perspective. This underpins the importance of accountability in the use of artificial intelligence, including the use of facial recognition technologies.

I don't think it's too late.

[*Translation*]

Mr. René Villemure: Thank you, Ms. Piovesan. I'll continue with you, if I may.

About two months ago, the Superior Court of Quebec handed down a decision on Clearview AI, asking that the company return the data it holds or destroy it. Clearview AI simply refused, adding that it is not in Canada and we have no authority over it.

What is done in cases like this?

[*English*]

Ms. Carole Piovesan: The extra-jurisdictional enforcement of these types of decisions is very difficult. We've seen this raised by courts before. We draw inspiration from the General Data Protection Regulation out of the EU that is starting to impose very significant fines, not for actual activity in the European jurisdiction, but for the use of European data subjects—the use of data of European residents.

Opportunities to extend jurisdiction and enforcement are being very much explored. We've seen this in Quebec, absolutely, with the passing of new private sector reform of the privacy law. It is certainly a consideration that we saw in the old Bill C-11, which was to reform aspects of PIPEDA. We'll see what comes out of the new reform, when and if it comes.

● (1130)

[*Translation*]

Mr. René Villemure: Thank you very much.

You talked about a holistic approach in a recent interview. Could you elaborate on that?

[*English*]

Ms. Carole Piovesan: Absolutely.

When we're looking at the regulation of artificial intelligence, we need to look at aspects of the data, as well as the use and the design of the technology to ensure that it is properly regulated. In different jurisdictions, including the United States and the EU, we see an attempt to regulate artificial intelligence—including facial recognition very specifically—that takes a risk-based approach to the regulation.

If we draw inspiration from the EU's draft artificial intelligence act, we see that a criticality of risk is first anticipated, which means there are some use cases that are considered prohibitive or very high-risk. Others are considered high-risk categories for regulation and then the risk level decreases.

The high-risk categories are specifically regulated with a more proscriptive pen, telling both vendors and users of those systems what some of the requirements are and what needs to be done to verify and validate the system and the data, and then imposes ongoing controls to ensure that the system is operating as intended.

That is a really important point because when you are using a high-risk AI system—recognizing that artificial intelligence is quite sophisticated and unique in its self-learning and self-actioning embodiment—having those controls after the fact is really critical to ensure that there is an ongoing use.

The Chair: Thank you.

[*Translation*]

Mr. René Villemure: Thank you very much.

[*English*]

The Chair: We're just a little over the time limit.

I'd now like to go to Mr. Green for six minutes.

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

I want to begin by acknowledging that today is March 21, which marks the International Day for the Elimination of Racial Discrimination. It was some 60 years ago, in 1960, in fact, when the Sharpeville police massacre happened in South Africa against workers.

I want to take a step back from the specificity around the tools and talk about the systems for a moment, and draw a direct line between what I believe occurred under C-51 and the implementation of anti-terrorism protocols provincially that led to the analog version of facial recognition, which was the practice of street checks and racial profiling, otherwise known as “carding” by local police services. I'll pick up from there, because I believe that practice of racial profiling, the analog version, has been in a very sophisticated way ruled out and then reimplemented as has been identified here through private sector contracts that allow companies like Clearview to do indirectly what police services were doing directly.

I want to also situate the conversation in the system, which is this notion of predictive policing as the basis of my questions, because I believe that the topic of facial recognition may be overly broad to get any kind of real coverage on this.

My questions will be to Ms. Khoo, who had laid out in an extensive report some of the bases for recommendations moving forward. I would like Ms. Khoo to comment on the evolution of predictive policing, its inherent racial bias and this notion of creating de facto panoptic prisons within our communities that are often over-surveilled, over-policed and underserviced.

Ms. Khoo, would you care to comment on that, and perhaps draw any lines that you may have come across between the practices of street checks and carding to populate data in things like CPIC, which would obviously be replaced by more sophisticated data such as AI and facial recognition?

● (1135)

Ms. Cynthia Khoo: Thank you very much for that question. I'm just trying to compile all my thoughts, because there are many issues that could fall under the umbrella you set out.

The first point I would make is that you're absolutely right in tracing that line. That's something we heard from a lot of the racial justice activists we talked to in the research for our report. For them, this is just 21st century state violence. It used to be done with pen and paper, and now it's done with computers and algorithms.

We're trying to move away from the term “predictive policing” just because, by this point, it's more of a marketing term and suggests a lot more certainty than the technology can really promise, because it's been popularized and it's what people know. One way that highlights the racial justice history behind it is asking if this would still be a problem if the technology worked perfectly. Our answer would be to look at what it's being used for. It's used for break and enters and so-called street crime and property crime. You will only ever catch a particular type of person if you're looking at a particular type of crime.

There's this great satirical project that makes a very compelling point in New York. They published something that they called the “white collar” crime heat map. That is essentially a crime heat map that only focuses on the financial district of downtown Manhattan. So, why are there not venture capitalists rushing to fund the start-up to create that type of predictive policing? It's because even if it worked perfectly, it still only enures to the benefit and detriment of particular social groups that fall along historical lines of systemic oppression.

The second point is I'm really happy that you brought up the “zooming out” contextualization of these technologies, because I believe in the next panel, you will be talking to Professor Kristen Thomasen, who is a colleague of mine. I would highly encourage you to pay attention to her comments, because she primarily focuses on situations in these technologies in the broader context of their being a socio-technical system and how you can't look at them divorced from the history that they're in. Even in Brazil, there was a rising field within the algorithmic accountability field that looked at the idea of critical algorithmic accountability or critical AI. They looked at what would it look like to decolonize artificial intelligence studies, for example, or to centre these historically marginalized groups even among the data scientists and the people who are working on these issues themselves.

I think I had one or two other thoughts, but maybe I'll stop there for now.

Mr. Matthew Green: With my remaining minute, I recall, as a city councillor, taking on the process of street checks and racial profiling. Through FOIs, as a city councillor, I came across an internal memo from the Ontario Ministry of the Attorney General which, under the anti-terrorism protocol, stated that street checks provided a unique opportunity for the mass collection of data.

I reference our own local Hamilton Police Service's use of Clearview. I reference many times when wrongful identity scenarios happened and the lawsuits that happened in response. I reference their constant refrain on this topic of predictive policing.

The first time I heard that was at a business planning session with the Hamilton Police. All I could think about was *Minority Report* and how terrifying that was as a sci-fi social commentary some 20 years ago. Here we are today.

Thank you.

The Chair: We'll go to the next round of five minutes with Mr. Kurek.

Go ahead.

Mr. Damien Kurek (Battle River—Crowfoot, CPC): Thank you very much. I appreciate the testimony that was provided and the questions that have been asked.

This whole discussion, be it on facial recognition or artificial intelligence, is really touching on what is a Pandora's box of massive implications in our society, law enforcement and technology. In reading on this subject, you see everything from how we log into our phones to evidence that's being compiled without consent for criminal prosecutions.

My hope is to get a couple of questions in to both of you. My first question surrounds the interplay between the state and private corporations and, sometimes, the contracts by which state actors— whether they be police forces or otherwise— will engage private corporations.

Ms. Khoo can answer first. Do you have specific recommendations about what regulations should look like to ensure that Canadians' privacy is protected in this case?

● (1140)

Ms. Cynthia Khoo: I will start with three recommendations.

The first one is that if law enforcement is considering adopting facial recognition technology or algorithmic policing technology, it's a very real option for them not to engage with a commercial vendor at all. For example, Saskatchewan Police's protective analytics lab built all of their technology in-house, specifically to avoid these kinds of problems and being beholden to proprietary interests. It's publicly funded technology. It's all run by the province, the University of Saskatchewan and the municipal police force. That doesn't mean that there are no problems, but at least it cuts out the problems that would be associated with being tied to a commercial vendor.

The second thing is that, if you are going to procure from a commercial vendor, we would suggest putting in several really strict upfront procurement conditions. An example would be not accepting contracts with any company that has said it's not willing to waive its trade secrets for the purposes of independent auditing and making sure that it is contractually bound to comply with public interest privacy standards.

The third way to protect privacy and ensure public accountability is by ensuring less secrecy around these contracts. We shouldn't be finding out about them after the fact, through leaks, persistent FOIs or investigative journalists. We should know about them before they happen, when they're still at the tender stage, and have an opportunity to comment on them.

Mr. Damien Kurek: Thank you very much.

Ms. Piovesan, do you have anything to add?

Ms. Carole Piovesan: I very much agree with Ms. Khoo's comments.

I would add that there is an element of stakeholder engagement as well. We need to be able to reach out to the community, particularly those affected, and have a meaningful discussion about how these technologies are used and what the implications of these technologies are before they're rolled out.

We've often heard about the concept of radical transparency. When we're talking about something as profound as facial recognition technology, applying and adopting a concept of radical transparency can be extremely helpful.

Also, underscoring the point of explainability, will we be able to understand how these algorithms operate? Will we able to understand the output they provide, and can we have independent verification to ensure that they are accurate and reliable?

Mr. Damien Kurek: Thank you for that.

It's interesting. I have an article in front of me where the headline is “Toronto police used Clearview AI facial recognition software in 84 investigations”, and the byline has in part “At least 2 cases went to court”. This is something that is not just theoretical; it is actually happening.

Especially as we are faced with a war in Europe and some of the discussions around what facial recognition and artificial intelligence look like in a military context, when you think about the Geneva Convention, it has to do with bombs that are dropped from airplanes. However, this is a whole new space with massive consequences.

I've had a whole host of constituents who have reached out with concerns about digital ID, the social credit system and some of the challenges that are associated with the state tying your information to aspects of your interaction with the government. I'm wondering if both of you, hopefully—

I'm out of time.

The Chair: You're going to have to allow the witness about 15 seconds for a reply. Then we'll have to pick it up in another round.

I'm not sure which witness wants to weigh in there for a quick moment to address his questions.

Ms. Cynthia Khoo: I think we thought he was done. Maybe we'll try again in the next round.

The Chair: All right. We'll hold that thought.

I will go now to Ms. Hepfner.

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

Thank you, witnesses, for your testimony this morning. It's been really interesting and I think really technical. I might sound a little bit repetitive, but I want to make sure I understand your points of view.

I want to start with PIPEDA. We know that the government is looking at this digital policy framework right now and trying to adapt it. It was developed before facial recognition software existed. I'm wondering if both of you can comment on exactly what sorts of improvements you'd like to see in that legislation. How can we make that legislation more adaptive to these technologies? It won't be the last new technology that we have to deal with. These things keep coming up, and the legislation doesn't keep pace. I'm wondering if you have ideas about how to make it more flexible so that when new technologies like this come into our society, we're more able to deal with the privacy concerns.

Maybe we'll start with Ms. Khoo.

● (1145)

Ms. Cynthia Khoo: I think when it comes to improving PIPEDA, the number one thing, the most important thing that I think a lot of privacy advocates have been calling for since the creation of PIPEDA, is to fix the enforcement piece. There are a lot of cases where PIPEDA, in terms of its legal content and what it does and doesn't allow, would not in fact allow the activity that occurs.

When it came to Facebook and Cambridge Analytica, for example, that was found illegal under PIPEDA. When it came to Clearview AI, they successfully.... PIPEDA captured that activity, but it was the fact that the OPC didn't have the power to then issue orders. They would have had to drag the company into court. They don't have the power to issue fines, let alone fines at the level of the GDPR.

I think the single most impactful change that could be made would be to give the Office of the Privacy Commissioner of Canada some teeth to actually enforce the orders against companies that are already found to be engaging in illegal activity under PIPEDA, or what comes after PIPEDA.

Ms. Carole Piovesan: I would agree on the enforcement point. I think what was interesting under Bill C-11 was that it contemplated a tribunal that would oversee, and potentially have more serious consequences over, specific violations of the act. It's something that I'm hoping we'll continue to see in the next round.

Another point that we saw to an extent in Bill C-11 was a broadening of various elements of consent as a basis for collecting, using and disclosing personal information. Again, we have to be mindful that PIPEDA is a private sector privacy law. We have to be mindful of some of the positive uses of facial recognition technology, which is why I say it has to be regulated using a scalpel, not an axe. There are some very beneficial uses, but we need appropriate safeguards to ensure that those uses are properly controlled and contained and that they feed the public interest and don't subvert our values. It's very important that we see that in whatever new reform to PIPEDA we ultimately get.

Ms. Lisa Hepfner: Thank you very much.

That fits perfectly into my next question—namely, what are the societal benefits that we can see from this technology? We've heard a lot about the privacy and discrimination concerns. Other than obviously the commercial benefits to the companies that have this software, what are the societal benefits to this sort of software?

Ms. Carole Piovesan: I'm happy to start. I referenced the use of facial recognition in health care, where we have seen some examples of FRTs being used to monitor patients and make sure their well-being isn't changing, particularly if they're on bed rest and may not be vocal. We've seen some very positive uses of FRTs in the health care sector. Of course, we would want to be very cautious about both the collection and the use of that technology. The retention of that data is very important. The limited disclosure of that data is extremely important. But we can see that there are some very notable positive benefits when you look at it in the health context.

I personally use facial recognition to unlock and verify my identity for my bank and my phone. Again, we want strict controls in place. We see it as a convenience. Is it a necessary convenience? No, not necessarily, but it can be a very secure way to go through a payment process or an airport, or to conduct a financial transaction.

There can be positive societal benefits. The issue becomes whether or not there is appropriate disclosure and notice on the collection of that data and how it will be used. Then, is there an appropriate retention period that is ultimately in the control of the individual? That is exactly what PIPEDA is intended to do, to wrest some of that control over informational privacy back into the hands of users, with appropriate—

The Chair: I'm going to have to move on. We're getting very close on time here. Thank you for that response.

I will go now to Monsieur Villemure.

[*Translation*]

You have two and a half minutes.

Mr. René Villemure: Thank you, Mr. Chair. Two and a half minutes go by very quickly.

Ms. Piovesan, I will address you again.

You referred to the general data protection regulation, or GDPR. I would like to know what GDPR best practices we could draw on.

At the same time, there was talk of consent being difficult to obtain, but at the end of the day, is it impossible to obtain it?

● (1150)

[*English*]

Ms. Carole Piovesan: You know, consent can be very difficult, depending on the use case, particularly the scalability of facial recognition technology, but it should not be thrown out as a requirement just in and of itself. We need to include consent as a key requirement. We are talking about an immutable biometric data point on an individual. Having appropriate notice, with some ability for that individual to make decisions about how they share that information or how it's collected, is really critical. I don't want to suggest that consent should never be a consideration when you're talking about facial recognition technology. That's absolutely not true.

When we look at GDPR, we can certainly draw inspiration from the profiling requirements that I know Quebec has done in terms of looking at a right to recourse and a right to objection on automatic profiling solely by automatic means. That's one element that we should consider, but again, I very much encourage the committee to look at the EU's artificial intelligence act. It's not final, but there is some real inspiration that we can draw from there. The draft algorithmic accountability act out of the U.S. is worth looking at as well.

[*Translation*]

Mr. René Villemure: Okay.

Tell me a little more about radical transparency.

[*English*]

Ms. Carole Piovesan: Radical transparency really speaks to the entire disclosure process—to allowing people, putting it out there, letting people know who your vendors are, what your uses are, where you are collecting that data and why you are doing so. It's very much about engaging the public as opposed to, as you heard Ms. Khoo mention a number of times, this concept of secrecy that undermines the trust we already have. It also starts to subvert some of those really important Canadian values.

Radical transparency is starting with the principle that we are going to get out there and let our constituents know what we're doing with facial recognition, or any type of really advanced technology that can impact on their rights, bring them into the discussion in a meaningful way, and then report on some of those outputs, including reporting on vendor relationships.

[*Translation*]

Mr. René Villemure: Thank you very much.

[*English*]

The Chair: Thank you.

There are two and a half minutes for Mr. Green.

Mr. Matthew Green: Thank you.

I want to pick up on a topic that my colleague from the Bloc has raised on occasion and that I share an interest in, and that's surveillance capitalism. My questions are for Ms. Khoo on the relationship between private companies. We referenced Clearview. There are others that we know of, including Amazon. We even know that Ring technology for doorbells provides an opportunity to privatize and capitalize on public space surreptitiously, without the knowledge of people.

I wonder if you could comment on that, and after that talk about the susceptibilities for abuse by both the private sector and government. I think about the ways in which it's used voyeuristically. You brought up the gender-based analysis there.

I'm wondering if you could just touch on those two topics.

Ms. Cynthia Khoo: Absolutely. Thank you.

In terms of capitalizing on public space, this is something we are definitely concerned about. Amazon Ring is actually the poster child for that. To my knowledge, it has not come up here yet. Again, Professor Thomasen can speak more to this. I think Amazon Ring was looking at Windsor at one point.

We know that there are open partnerships—well, now there are open partnerships—between Amazon and police. Police were essentially conscripted as the marketing department of Amazon Ring doorbells, which raises numerous concerns from the perspective of both the private sector and the public sector, but mostly the public sector.

Surveillance capitalism is an aspect of this public-private surveillance ecosystem, because it has to do with incentive structures. You have the private companies with their own incentives to collect as much data as possible to capitalize on it. A lot of their funding then comes from government through government grants. Whether it's through the guise of innovation or whether it's because they have lobbied government behind the scenes to give them these particular grants, the government funds them. It's partly because they buy into an innovation story or they think, hey, if the company collects all this data, then maybe eventually we'll have access to that data too. It's essentially government and private companies working hand in hand to build out this network of surveillance.

The second thing you mentioned was abuse. I think we have so many examples of that. Actually, in responding to the earlier question about the potentially beneficial uses of facial recognition technology, my mind went to—

● (1155)

The Chair: I'm really sorry, but I'm going to have to cut you off just to get the last two rounds in. Perhaps, hold your thoughts.

I have to shorten the last two rounds. We'll go to three minutes each for Mr. Bezan and Ms. Khalid.

Mr. James Bezan (Selkirk—Interlake—Eastman, CPC): Thank you, Mr. Chair. That's unfortunate, because I have a lot of questions.

I thank both of our witnesses for their great testimony.

Let's start with Ms. Khoo. You and Kate Robertson sent a letter off to the Privacy Commissioner of Canada back on October 22, 2021. Did you get a response to that letter, and if you did, can you share it with the committee?

Ms. Cynthia Khoo: To my knowledge, I don't think we got a response, but I'll double-check with my colleague Kate Robertson and we can follow up with you.

Mr. James Bezan: Okay, please do, because I really believe the stuff that you have in there, talking about three parts as to algorithmic policing technologies. You talk about the moratoriums, ask that the federal government have a judicial inquiry, and that governments must make reliability, necessity and proportionality prerequisite conditions, as well as transparency, more directives on algorithmic policing technologies, or predictive policing—which is even scarier—and so on.

You talk in the letter about “the worst human rights and charter violations that could occur as a result of Canadian government and law enforcement agencies using algorithmic police technologies.” You want to mitigate that.

How do we, as parliamentarians, do that as we go forward in wanting to write the proper regulations that respect our charter rights and ultimately bring that balance of transparency, of people's ability to opt in and opt out, and maximize on the technology that's coming down the pipe at us?

Ms. Cynthia Khoo: As parliamentarians, the first thing you could do and our first recommendation is to launch an inquiry, essentially, or a national commission into these technologies.

For the purpose of this committee, my recommendation was a moratorium on facial recognition, but in that report we actually called for a moratorium on all algorithmic policing technologies pending the results of that inquiry, whether it's a national commission or a judicial inquiry, to do a much more in-depth constitutional and human rights analysis than we were able to do within our reports, so that you actually are able to lay out the contents of what's appropriate and what's not and what safeguards are required, and then actually implement them.

Without doing that, this train is moving ahead in the meantime. We need a national pause to buy ourselves time to figure out what to do with this technology so that we don't realize it way after the fact.

Mr. James Bezan: The Privacy Commissioner would have the ability to bring about that pause if we believe people's privacy rights are going to be violated, so that buys us that time to do the evaluation.

How many police agencies in Canada are using facial recognition technology?

Ms. Cynthia Khoo: That's a great question.

If you're looking at Clearview AI, I believe it was several dozen that were testing Clearview AI. However, for the purposes of our report, in terms of who were really using it, we found that it was the Toronto Police Service and the Calgary Police Service.

I saw last month that the Edmonton Police Service signed a contract. This was not with Clearview AI; this was with NEC Corporation, so it's separate facial recognition technology.

In our report, we saw York and Peel had announced that they were planning to engage in contracts too.

The Chair: Thank you, I'm going to have to go on, but that's a great question and if you have additional specific information on that, that's something that would probably be very helpful to our analysts in the preparation of the report.

With that, we'll finish this with Ms. Khalid for three minutes.

Ms. Iqra Khalid (Mississauga—Erin Mills, Lib.): Thank you very much, Chair; and thank you, witnesses, for your very compelling testimony today.

In the interest of time, I'll just ask Ms. Piovesan. We see on Facebook, when you log in, you put up a photo of yourself and your friends, and all of sudden, when you go to tag it, there's a list of potential people who that could be, and nine times out of 10, it is accurate. When we have these social media platforms and their use of facial recognition and their algorithms, they create these circles or bubbles of societies and we've seen how that commercial aspect of it has an impact on that discrimination and creating extreme views, and so on.

Could you maybe comment on that commercial aspect? How do we narrow that scope to make sure that businesses are able to efficiently provide services to consumers without consumers then becoming sheep to be led down a certain path, not just in terms of products but also ideologies?

● (1200)

Ms. Carole Piovesan: I have four quick proposals.

The first is that we need to have a risk assessment of the systems conducted to understand where the risks, the potential unintended consequences and foreseeable harms are.

That also leads to an impact assessment where you have to look specifically at what the potential impacts of this system are on individuals, on property and on rights. Have that be a thorough assessment, as we already see in the privacy space and as you heard Ms. Khoo refer to as an algorithmic impact assessment that is already adopted by the federal government.

Next, there needs to be clear and plain disclosure so people can make decisions in the commercial context in particular. Often it's not a need to have; it's a nice to have. People need to have that opportunity to understand how their information will be used, not through 20-page privacy policies—which I myself write all the time—but through clear and plain just-in-time information so that they can make and change their decisions and their consent if they choose not to continue. If they had agreed to provide their face originally, they have the right to change that over time.

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

I realize that I have 20 seconds, but Ms. Khoo, do you want to comment on that?

Ms. Cynthia Khoo: I have nothing further to add, but I will use that time to recommend the work of Simone Browne in reference to Mr. Green's earlier comments on racial justice. She wrote a book called *Dark Matters*, which traces biometric surveillance back to trans-Atlantic slavery and the branding of slaves. It argues that this was the origin of biometric surveillance.

The Chair: Thank you very much to our witnesses.

With that we will briefly suspend.

Mr. Matthew Green: Mr. Chair, before the suspension, through you to the witnesses, could I ask if there is anything they feel they didn't get a chance to fully answer, to please provide it to this committee in writing for the consideration of reports?

I am remiss and I share the concerns [*Inaudible—Editor*].

The Chair: Yes, you may do so and you have done so now.

Thank you, Mr. Green.

As a general comment to members, when you ask a complicated question and leave 10 seconds for the response, you put me in the awkward position of having to cut off our witness. Manage your time so you can get the answers in rather than just your questions.

With that we'll suspend—

Mr. Matthew Green: Mr. Chair, complicated topics have complicated questions.

If the witnesses can provide their expanded answers that would be great for the consideration.

● (1205)

The Chair: I agree one hundred per cent.

With that, we will briefly suspend while we transition the panels.

● (1205)

_____________________(Pause)_____________________

● (1205)

The Chair: The meeting has resumed.

I encourage everyone in the room to take their seats and keep the side discussion down so we can get started. Thank you.

We're getting pressed for time already. I'm going to start off with our opening statements. I'm going to ask our witnesses to keep to an absolute maximum of five minutes. I'm going to have to cut everyone off right when we get to that point.

Today, we have as individuals Ms. Ana Brandusescu, artificial intelligence governance expert; Kristen Thomasen, professor at University of British Columbia, Peter A. Allard School of Law; and Petra Molnar, associate director at the Refugee Law Lab.

We'll begin with Ms. Brandusescu.

You have an absolute max of five minutes.

Ms. Ana Brandusescu (Artificial Intelligence Governance Expert, As an Individual): Good afternoon Mr. Chair and members of the committee. Thank you for having me here today.

My name is Ms. Ana Brandusescu. I research governance and procurement of artificial intelligence technologies, particularly by government. That includes facial recognition technology, or FRT.

I will present two issues and three solutions today. The first issue is discrimination. FRT is better at distinguishing white male faces than Black, brown, indigenous and trans faces. We know this from groundbreaking work by scholars like Joy Buolamwini and Timnit Gebru. Their study found that:

> ...darker skinned females are the most misclassified group (with error rates of up to 34.7%). The maximum error rate for lighter-skinned males is 0.8%.

FRT generates lots of false positives. That means identifying you as someone you're not. This causes agents of the state to arrest the wrong person. Journalist Khari Johnson recently wrote for Wired about how in the U.S., three Black men were wrongfully arrested because they were misidentified by FRT.

Also, HR could deny someone a job because of FRT misidentification or could get an insurance company to deny a person coverage. FRT is more than problematic.

The House of Commons Standing Committee on Public Safety and National Security's report from 2021 states that there is systemic racism in policing in Canada. FRT exacerbates systemic racism.

The second issue is the lack of regulatory mechanisms. In a report I co-authored with privacy and cybersecurity expert Yuan Stevens for the Centre for Media, Technology and Democracy, we wrote that “as taxpayers, we are essentially paying to be surveilled, where companies like Clearview AI can exploit public sector tech procurement processes.”

Regulation is difficult. Why? Like much of big tech, AI crosses political boundaries. It can also evade procurement policies, such as Clearview offering free software trials. Because FRT is embedded in opaque, complex systems, it is sometimes hard for a government to know that FRT is part of a software package.

In June 2021, the Office of the Privacy Commissioner, OPC, was clear about needing system checks to ensure that the RCMP legally complies when using new technologies. However, the RCMP's response to the OPC was in favour of industry self-regulation. Self-regulation—for example, in the form of algorithmic impact assessments—can be insufficient. A lot of regulation vis-à-vis AI is essentially a volunteer activity.

What is the way forward? Government entities large and small have called for a ban on the use of FRT, and some have already banned it. That should be the end goal.

The Montréal Society and Artificial Intelligence Collective, which I contribute to, participated in the 2021 public consultation for Toronto Police Services Board's draft AI policy. Here, I extend some of these recommendations along with my own. I propose three solutions.

The first solution is to improve public procurement. Clearview AI got away with what it did across multiple jurisdictions in Canada because there was never a contract or procurement process involved. To prevent this, the OPC should create a policy for the proactive disclosure of free software trials used by law enforcement and all of government, as well as create a public registry for them. We need to make the black box a glass box. We need to know what we are being sold. We need to increase in-house AI expertise; otherwise, we cannot be certain agencies even know what they are buying. Also, companies linked to human rights abuses, like Palantir, should be removed from Canada's pre-qualified AI supplier list.

The second solution is to increase transparency. The OPC should work with the Treasury Board to create a public registry, this time for AI, and especially AI used for law enforcement and national security purposes, and for agencies contemplating face ID for social assistance, like employment insurance. An AI registry will be useful for researchers, academics and investigative journalists to inform the public. We also need to improve our algorithmic impact assessments, also known as AIAs.

AIAs should more meaningfully engage with civil society, yet the only external non-governmental actors consulted in Canada's three published AIAs were companies. The OPC should work with the Treasury Board to develop more specific, ongoing monitoring and reporting requirements, so the public knows if the use or impact of a system has changed since the initial AIA.

The third solution is to prioritize accountability. From the inside, the OPC should follow up on RCMP privacy commitments and demand a public-facing report that explains in detail the use of FRT in its unit. This can be applied to all departments and agencies in the future. From the outside, the OPC and the Treasury Board should fund and listen to civil society and community groups working on social issues, not only technology-related issues.

Thank you.

● (1210)

The Chair: Thank you very much.

With that, we'll go to Ms. Kristen Thomasen. You have five minutes.

Professor Kristen Thomasen (Professor, Peter A. Allard School of Law, University of British Columbia, As an Individual): Thank you, Mr. Chair, and thank you to the committee.

I am joining you from the unceded territory of the Squamish, Tsleil-Waututh and Musqueam nations.

As you heard, I'm a law professor, and my research focuses on the domestic regulation of artificial intelligence and robotics, especially as this relates to public spaces and privacy. I'm representing my own views here today.

I'm very grateful to the committee for the invitation to contribute to this important study. I urge this committee to supply a substantive equality lens to your report and all recommendations made to the government.

Much research has already shown how inequitable various forms of facial surveillance can be, particularly with respect to the misidentification of individuals on the basis of race, gender and age and the quality and source of data used to train such systems. However, even perfectly accurate facial surveillance systems built on data reported to be legally sourced can reflect and deepen social inequality for a range of reasons. I'll focus on some key points and welcome further questions later, including related to apparent narrow beneficial use cases.

First, facial surveillance systems are socio-technical systems, meaning that these technologies cannot be understood just by looking at how a system is built. One must also look at how it will interact with the people who use it, the people affected by it and the social environments in which it is deployed.

Facial surveillance consolidates and perfects surveillance and is introduced into a society where, for example, the Supreme Court of Canada, among other, has already recognized that communities are over-policed on the basis of protected identity grounds. Equity-seeking groups face greater quantities of interpersonal, state and commercial surveillance, and can experience qualitatively greater harm from that surveillance. More perfect surveillance means greater privacy harm and inequity.

I urge the committee to explicitly consider social context in your report and recommendations. This includes that biometric surveillance is not new. I encourage you to place facial surveillance within its historical trajectory, which emerged from eugenic and white supremacist sciences.

Part of the socio-technical context in which facial surveillance is introduced includes gaps in the application and underlying theories of laws of general application. In other words, our laws do not adequately protect against misuses of this technology. In particular, from my own research, I would flag that interpersonal uses of facial surveillance will be under-regulated.

I'm very encouraged to see that the committee is considering interpersonal use within the scope of this study and urge the committee to examine the interrelations between interpersonal surveillance and commercial and state entities. For example, while not specific to facial surveillance, the emergence of Amazon Ring-police partnerships in the United States highlights the potential Interweb of personal surveillance, commercial surveillance infrastructure and state policing, which will at least present challenges to current tort and constitutional laws as interrelations like this emerge in Canada.

Personal use facial surveillance has already been shown to be highly damaging in various cases, particularly with respect to technology-facilitated harassment, doxing and other forms of violence. These uses remain under-regulated because interpersonal surveillance in public spaces and public information is under-regulated. While governance of interpersonal privacy may not fall exhaustively within federal jurisdiction, I do think this is a crucial part of understanding facial surveillance as a socio-technical system and must be considered within the governance of such a technology. I also do not think the solution is to criminalize the personal use of facial surveillance systems, but rather to bolster normative and legal recognition of interpersonal rights and to regulate the design and availability of facial surveillance technologies.

Laws and policies governing technology can have at least three foci: regulating the uses of the technology, regulating the user, and/or regulating the design and availability of the technology. Regulation of design and availability may fall more directly within federal government jurisdiction and better focuses on those responsible for the creation of the possibility of such harm rather than only reactively focusing on punishing wrongdoing and/or compensating for harm that has already occurred.

Also, in terms of regulating the use of facial surveillance, I urge the committee to look to examples around the world where governments have adopted a moratorium on the use of facial surveillance, as has been mentioned by other witnesses, and I do also recommend the same in Canada. More is of course needed in the long term, including expanding the governance focus to include all forms of automated biometric surveillance, not exclusively facial surveillance. The committee may also consider recommending the creation of a national independent expert group to consult on further refinement of laws of general application and design use and user restrictions going forward, perhaps for both federal and provincial guidelines.

● (1215)

Expertise must include those—

The Chair: Thank you.

Prof. Kristen Thomasen: —from the impacted communities.

Thank you.

The Chair: I'm really sorry, Ms. Thomasen, that I have to cut you off there. We need to go to our third panellist.

Ms. Molnar, you have five minutes

Dr. Petra Molnar (Lawyer, Refugee Law Lab, York University): Thank you so much.

My name is Petra Molnar. I'm a lawyer and an anthropologist. Today I would like to share with you a few reflections from my work on the human rights impacts of such technologies as the facial recognition used in immigration and for border management.

Facial recognition technology underpins many of the types of technological experiments that we are seeing in the migration and border space, technologies that introduce biometric mass surveillance into refugee camps, immigration detention proceedings and airports. However, when trying to understand the impacts of various migration management and border technologies—i.e., AI lie detectors, biometric mass surveillance and various automated decision-making tools—it is important to consider the broader ecosystem in which these technologies develop. It is an ecosystem that is increasingly replete with the criminalization of migration, anti-migrant sentiments, and border practices leading to thousands of deaths, which we see not only in Europe but also at the U.S.-Mexico border, and most recently at the U.S.-Canada border, when a family froze to death in Manitoba.

Since 2018 I have monitored and visited borders all around the world, most recently the U.S.-Mexico frontier and the Ukrainian border during the ongoing occupation. Borders easily become testing grounds for new technologies, because migration and border enforcement already make up an opaque and discretionary decision-making space, one where life-changing decisions are rendered by decision-makers with little oversight and accountability in a system of vast power differentials between those affected by technology and those wielding it.

Perhaps a real-world example would be instructive here to illustrate just how far-reaching the impacts of technologies used for migration management can be. A few weeks ago, I was in the Sonoran Desert at the U.S.-Mexico border to see first-hand the impacts of technologies that are being tested out. These technological experiments include various automated and AI-powered surveillance towers sweeping the desert. Facial recognition and biometric mass surveillance, and even recently announced “robodogs”—like my barking dog in the background—are now joining the global arsenal of border enforcement technologies.

The future is not just more technology, however; it is more death. Thousands of people have already perished making dangerous crossings. These are people like Mr. Alvarado, a young husband and father from Central America whose memorial site we visited. Indeed, surveillance and smart border technologies have been proven to not deter people from making dangerous crossings. Instead, people have been forced to change their routes towards less inhabited terrain, leading to loss of life.

Again, in the opaque and discretionary world of border enforcement and immigration decision-making, structures that are underpinned by intersecting systemic racism and historical discrimination against people migrating, technology's impacts on people's human rights are very real. As other witnesses have already said, we already know that facial recognition is highly discriminatory against black and brown faces and that algorithmic decision-making often relies on biased datasets that render biased results.

For me, one of the most visceral examples of the far-reaching impacts of facial recognition is the increasing appetite for AI polygraphs, or lie detectors, used at the border. The EU has been experimenting with a now derided system called iBorderCtrl. Canada has tested a similar system called AVATAR. These polygraphs use facial and emotional recognition technologies to reportedly discern whether a person is lying when presented with a series of questions at a border crossing. However, how can an AI lie detector deal with differences in cross-cultural communication when a person, due to religious or ethnic differences, may be reticent to make eye contact, or may just be nervous? What about the impact of trauma on memory, or the fact that we know that we do not recollect information in a linear way? Human decision-makers already have issues with these complex factors.

At the end of the day, this conversation isn't really about just technology. It's about broader questions. It's about questions around which communities get to participate in conversations around proposed innovation, and which groups of people become testing grounds for border technologies. Why does the private sector get to determine, time and again, what we innovate on and why, in often problematic public-private partnerships, which states are increasingly keen to make in today's global AI arms race? Whose priorities really matter when we choose to create AI-powered lie detectors at the border instead of using AI to identify racist border guards?

In my work, based on years of on-the-ground research and hundreds of conversations with people who are themselves at the sharpest edges of technological experimentation at the border, it is clear that the current lack of global governance around high-risk technologies creates a perfect laboratory for high-risk experiments, making people on the move, migrants and refugees a testing ground.

Currently, very little regulation of FRT exists in Canada and internationally. However, the European Union's recently proposed regulation on AI demonstrates a regional recognition that technologies used for migration management need to be strictly regulated, with ongoing discussions around an outright ban on biometric mass surveillance, high-risk facial recognition and AI-type lie detectors. Canada should also take a leading role globally. We should introduce similar governance mechanisms that recognize the far-reaching human rights impacts of high-risk technologies and ban the high-risk use of FRT in migration and at the border.

● (1220)

We desperately need more regulation, oversight and accountability mechanisms for border tech used by states like Canada.

The Chair: Thank you, Ms. Molnar.

I'm going to have to begin the questions. We're at 25 after 12. I am going to cut the six- and five-minute rounds to four minutes. With that, we should maybe end a few minutes after one o'clock.

I'm going to go to Mr. Williams for four minutes.

Mr. Ryan Williams: Thank you very much to our panellists.

I'll start with Ms. Brandusescu.

Last month you were part of a response to the Toronto Police Service's proposed policy on AI technology use, which included facial recognition. Section two talked about “explainability”, which was called an important step for “ensuring that AI technologies remain accountable to users and affected populations”. I also loved your definition of glass boxing the black box. It's very important.

Do we need to define “explainability” in federal legislation to ensure a universal application and understanding of the term? If so, how would you define it?

Ms. Ana Brandusescu: Thank you so much.

We will be told that explainable AI is a computational solution we're going to have to make sure FRT can go forward.

I want to argue that even though explainable AI is a growing field, it's actually adding more complexity, not less. This is because explanation is entirely audience dependent. That audience is usually comprised of computer scientists, not politicians.

Who gets to participate in that conversation and who's also left out is really important. It's not enough to have explainable AI even because of the neural network type of AI that FRT is. It can never be fully explained.

That is also part of our recommendation. In short, it is really trying to get to the core of what the technology is and understanding the black box. Having a technical solution to a very problematic technology doesn't mean we should use it to go forward and not consider the ban.

● (1225)

Mr. Ryan Williams: Thank you.

You had a 2021 paper called “Weak privacy, weak procurement: The state of facial recognition in Canada”. You talked about biometric data protection and how Canada's privacy laws are failing compared to the rest of the world.

We've heard of the benefits of the General Data Protection Regulation, GDPR, from a witness in a previous meeting. Would adopting a GDPR-style protection be better for Canada's privacy rights?

Ms. Ana Brandusescu: That was the lead of my co-author, Yuan Stevens, who focuses on privacy expertise. I will try to say that GDPR is a good gold standard to have for best practices so far.

I would just argue that this is more than data protection or privacy. This is a conversation about the private sector as well and their involvement in public governance. Right now, what we have in our regulation is just private regulation.

I could touch upon the algorithmic impact assessment and our own directive automated decision-making more deeply in a future question.

Mr. Ryan Williams: Thank you.

Ms. Thomasen, in a March 2020 article with the CBC, you were talking about the Windsor Police's use of Clearview AI's facial recognition tool. You said, “How do we know that, if the victim is even identified, that their information is going to be protected?” I think that is a key message as the matter of facial recognition becomes more and more widespread.

My question to you is essentially to help answer the question you posed in the CBC story. How do we make sure Canadians know that their information is protected?

Prof. Kristen Thomasen: To give some context to that question, that was engaging a narrative that arises often with respect to police use of facial surveillance, which is that we use it to protect...in this instance it was children from harm. We need to worry about the broader impact on privacy as a social good.

What I was getting at there was what—

The Chair: I'm afraid you really weren't left with enough time to answer that question. I'm going to have to cut it off and go to Ms. Saks.

Prof. Kristen Thomasen: I'm happy to submit a further explanation.

The Chair: Please, indeed, submit a written explanation if you have one available or if you'd like to provide one.

Go ahead Ms. Saks, for four minutes, please.

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

Mr. Williams might be pleased that I'm going to be stepping off a bit from his question.

I think we're all in agreement that more needs to be done in understanding the use of this technology and making sure that there's a robust consultation with all of those impacted by privacy and how it's used. A previous witness described it as needing to go through this with a scalpel and not with an axe. I appreciate the calls for a moratorium for us to be able to utilize that scalpel. It's an important metaphor.

Ms. Thomasen, in talking about the victims, I've heard a lot of the negative impacts. I don't disagree with them. I am someone who has been engaged in fighting human trafficking for many many years. I understand the impacts of migration and borders, and human trafficking's impact on both women and children, many of them from racialized minorities.

Is there not some wisdom in using the scalpel in this technology, so that we can effectively protect those who are victims of human trafficking, or children who are subject to assault or child pornography? Are there other tools that we need to find ways to protect them?

Is that not a consideration in this discussion?

● (1230)

Prof. Kristen Thomasen: Yes. Privacy is a social good that benefits everyone, including the women and children who are often engaged in the narrative of saying that one of the beneficial uses of facial recognition is to protect marginalized or victimized groups. It's very important to acknowledge those potential beneficial uses of facial recognition while nuancing that narrative considerably. In particular, we need to recognize the way in which the potential erosion of privacy as a social good will also harm women and children.

One beneficial use case of facial surveillance, as far as I understand it, is an example from Canada, called Project Arachnid. It might be helpful to the committee to speak to someone involved in that project. It's a very narrowly designed use case of facial surveillance, or facial recognition technology more specifically. I'd be happy to speak more about definitions in another question.

The specific goals and purposes for the creation of an in-house facial recognition system have been set very narrowly. That is quite distinct from the broader arguments or narratives that facial recognition should not be banned or limited in various ways because there can be, generally speaking, potentially positive use cases. It's far more important to balance the social positive good of privacy in those kinds of discussions.

I feel like I'm limited on time. I'd be more than happy to talk about it more.

Ms. Ya'ara Saks: I would like to try to get in one more question, if I may.

The Chair: You can have just one.

Ms. Ya'ara Saks: In December 2021, you gave a submission to the Toronto Police Service in regards to its consultations on the use of artificial intelligence technology. You made quite a number of recommendations in your submission. If you would like to, you may highlight one key recommendation here, but I would encourage you to then provide us with submissions in writing so that we may review them.

Prof. Kristen Thomasen: I'll happily do that.

That was a co-authored submission.

One key recommendation I would like to highlight right now is that this technology is not inevitable. The fact that it exists does not mean that it should exist or that we should be using it. It does not mean that we shouldn't limit it.

Pointing to some beneficial use cases should not be sufficient to limit our thinking around the potential harms that can arise from more widespread use of the technology. In particular, we should be thinking more about the interrelationships between how police services, corporate agencies and individuals might be working together to collect information for the purposes of carceral end goals.

The Chair: Thank you.

[*Translation*]

Mr. Villemure, you have four minutes.

Mr. René Villemure: I would like to ask a brief question of each of the three witnesses, in their order of appearance.

Ms. Brandusescu, does facial recognition technology mean the end of freedom?

[*English*]

Ms. Ana Brandusescu: I would say no, because we can ban facial recognition. The end of freedom is a very complex and dire question and statement. I would argue that, again, this isn't just about mass surveillance; it's about how our governments interact with industry, how they procure different software and they have no idea what they're purchasing—

[*Translation*]

Mr. René Villemure: I'm sorry for interrupting you, but my time is limited. We'll come back to it.

Ms. Thomasen, I ask you the same question.

[*English*]

Prof. Kristen Thomasen: I agree with previous witnesses: This is a complex question to answer quite straightforwardly.

I would also encourage that the committee consider beyond just facial recognition. There are all forms of different biometric recognition that feed into the conversation we're having today.

[*Translation*]

Mr. René Villemure: Thank you very much.

What do you think, Dr. Molnar?

[*English*]

Dr. Petra Molnar: I would just encourage a contextual specificity with regard to this question, particularly when we're talking about freedoms: for whom?

In immigration, of course, we're talking about an opaque and discretionary space that's already very high risk. In this instance, yes, it can definitely be very limiting.

[*Translation*]

Mr. René Villemure: Thank you.

Ms. Brandusescu, is facial recognition technology transforming the public space in terms of surveillance, as Dr. Habermas sees it?

[*English*]

Ms. Ana Brandusescu: Yes, I would argue that there is mass surveillance, but specifically also a discriminatory racist and sexist surveillance, as we know, because this tech is very discriminatory in the way it is on a very computational level. The more we accept it into society the more it will just be something that we get used to. I don't want to have that convenience.

There was a convenience point made earlier. Sometimes I say that convenience will be the end of us when we use it to open up our phones. The more it becomes part of our daily lives, the more we just think it's okay to have it, but actually, it isn't, because it can really harm certain individuals and groups. Sometimes it's okay to just not have that technology at all.

It's a bigger question to have. It's a question around digital literacy. We need to have these discussions, and actually we need to have the critical digital literacy to ask the right questions.

● (1235)

[*Translation*]

Mr. René Villemure: Thank you very much.

Beyond the identified biases, such as those related to race or age, the citizen who is not targeted by those biases nevertheless enters a world of surveillance, correct?

[*English*]

Ms. Ana Brandusescu: We can go ahead and talk about data analytics firms and Palantir and others that aren't even FRTs. The world of surveillance goes way beyond FRT, and that's a bigger question to have about our country's military-industrial complex and where these technologies even come from.

We need to again zoom out and look at the way that technology has taken over. We need to reflect on what tech solutionism means, on why we put so much money and funding in tech innovation specifically, and why we look at innovation as just being tech-prone, and not actually funding groups who work very hard on social issues to understand this technology, to create public awareness and also education on this.

I have an optimistic view of the future, even though I am very critical of this technology. We have to imagine, to think about how we can live without some of this technology, and we'll be fine.

The Chair: Thank you. I'm going to have to move now to Mr. Green for four minutes, please.

Mr. Matthew Green: Thank you.

I will begin with my question to Ms. Brandusescu. In your report "Artificial Intelligence Policy and Funding in Canada: Public Investments, Private Interests", one of your main findings is that the current government policy allows companies with links to human rights abuses to pre-qualify as government AI suppliers.

In your previous answer, you talked about the military-industrial complex. We've heard stories of companies that actually tout their technologies as being battle-tested.

Are you aware of any companies that have been pre-qualified as suppliers, not just for facial recognition but throughout AI and this whole spectrum, that have previously been implicated in human rights abuses?

Ms. Ana Brandusescu: Thank you for the excellent question.

Yes, I am aware. One such supplier is Palantir Technologies Inc., which is a data analytics company that worked with the U.S. government to plan mass arrests for nearly 700 people and the separation of children from their parents, causing irreparable harm. You can see the report of Amnesty U.S.A. on that from 2020, yet as I mentioned in my opening statement, Palantir has committed to Canada's algorithmic impact assessment and it's on that pre-qualified supplier list, seen as an ethical measure that supports responsible AI. To be committed to an AIA that's supposed to be ethical and then commit with another government these human rights abuses is very paradoxical and contradictory.

I ask our government, especially the Treasury Board, which manages that list, to reconsider as I mentioned, to get them off the list—and not just them, but others that I haven't looked into deeply about potential human rights abuses.

Mr. Matthew Green: What changes in our policy do you think are needed to ensure that a human rights lens is a part of our procurement process?

Ms. Ana Brandusescu: I think one is once we write, researchers, investigative journalists, whoever—because we're at this point where our open government isn't really open, we still have to file an access to information request and find all this information—we need you to hear us. So the government now knows that Palantir has caused human rights abuses or is linked to them. The list is growing, it's at around 105 companies now, and the government should take Palantir off the list. That's one simple step, but it's also then to think about who can commit to the AIA and what does AI really mean and who has input to the AIA. If it's just other companies that are engaged when an AIA is published, what does that say about the rest of Canada, not just the Canadian public, but affected groups, digital rights organizations, civil society bodies? Where are we in the conversation?

● (1240)

Mr. Matthew Green: This is important work.

Mr. Chair, through you to Ms. Brandusescu, how concerned should we be about the corporate capture in government's policy development for regulating AI and facial recognition in Canada? And with this in mind, can you describe who is setting the Canadian policy framework for AI and what the are consequences for those?

Ms. Ana Brandusescu: We should be really concerned.

My next four years of research as a Ph.D. student will be around the privatization of the states specifically with these technologies. I think this will just get bigger. As Ms. Molnar mentioned, public-private partnerships are a key point about procuring and deploying and developing and using these technologies. We need to make sure that we are in line with the Treasury Board, which is hosting all the responsible AI suites, but also look at others like Public Services and Procurement Canada, that really hold a lot of cards here but are rarely in these discussions. It's always either the Treasury Board and the OPC that are in the conversation. I never see the procurement people, but really they are a key component here to this conversation.

The Chair: Thank you.

With that, we'll move to Mr. Kurek for four minutes.

Mr. Damien Kurek: Thank you very much.

Just before I get into my questions, knowing that we are short on time here I would invite all of the witnesses here, if there are things that you didn't have a chance to address, to please feel free to send information to this committee. These are big questions with technical answers. Two, three or four minutes is certainly not enough time to see them appropriately addressed.

I certainly see one of the biggest challenges with addressing this is even just the evolution of the space of artificial intelligence and facial recognition. I'd mentioned in the previous round, with the conflict in Europe right now, the implications of this on how military uses some of this technology and the Geneva Convention, for example, deal with bombs that are dropped from planes, but there's a whole new space that's opened up.

Ms. Brandusescu, as this technology is being developed, in terms of research, government, private corporations, testing and understanding of the impacts on this technology and its impacts on society, do you have suggestions as to a path forward for this committee that would ensure that there is an appropriate understanding of what this means for Canadian citizens, and the fact that we are facing a world where AI and facial recognition become more and more part of our daily lives?

Ms. Ana Brandusescu: Again, I think we can push back on tech inevitability, and we can say no to some of this technology, but that also requires funding and resources for education around these technologies. A lot of these contracts are made behind closed doors. In industry-government relationships, the public-private partnerships sometimes involve universities and labs, but it's always for a private interest focus. You want to fund these technologies, to build them, and then to use them. You don't think about the consequences. Very little money, time and resources go into dealing with the mess these technologies create and the harm they create.

We need to make sure there's a balance in that and move away and reconsider what we think about innovation when we fund that, especially as taxpayers. We need to really branch out. Right now I would say that the innovation work has been captured by specifically tech innovations that are designed to develop and deploy these technologies first and ask questions later. We can see how much harm they have caused, and yet here we are still debating this.

I don't want us to have a Clearview AI case, so what do we do? The free trial software transparency is really important, because that is beyond FRTs. That goes to all those AI systems and technologies that the government uses. Nobody sees that information anywhere. If we can get that information there, especially for law enforcement and national security, who won't use those excuses to say they're covering trade secrets....

We need to go beyond that. Again, if we want to build trust with the government, we need to have that level of transparency to know even what they are procuring and using so that we can ask better questions.

● (1245)

The Chair: Thank you.

With that, we will go to Mr. Bains for four minutes.

Mr. Parm Bains (Steveston—Richmond East, Lib.): Thank you, Mr. Chair.

Thank you to our witnesses for joining us today. All of you, along with our previous panel, have highlighted the considerable amount of challenges we're facing here.

Ms. Thomasen, recently you participated in drafting some comments on the Toronto Police Services Board's proposed policy on AI technologies. The first recommendation is as follows:

> Any implementation of AI technologies by law enforcement needs to begin from the assumption that it cannot reliably anticipate all the effects of those technologies on policing or policed communities and act accordingly in light of these impacts.

I'm interested to know how often, in your view, governments should be reviewing the effects of AI technology used in policing.

Ms. Kristen Thomasen: Often; I know that in the draft policy that was ultimately adopted as a policy by the TPSB, the reviews will take place annually, which I think is a positive. I actually think that because of the way in which technology progresses, and the quantity of data that can be collected and utilized, even over the course of a year, that in practice, in a perfect world, would not be enough. Of course, reviews and audits take resources and time. I recognize that there are some practical limitations there.

But that's one police force in Canada. There are other police forces that we already know are using algorithmic policing technologies and are not engaging in these reviews, at least not to the extent that we are aware of publicly. There isn't necessarily the public oversight or transparency available.

So I think the TPSB policy is a step forward. It is a positive step, but even then I think it's not enough. There's still a lot that could be done. I think to the extent that the federal government could be involved in establishing some form of guidelines, and then of course oversight for federal-level police forces, that would be a positive step.

Mr. Parm Bains: Were your recommendations satisfactorily incorporated into the final version of the policy by the TPS?

Ms. Kristen Thomasen: I think the final policy did incorporate a number of recommendations that were made—there were a number of parties who contributed recommendations to that process—but there were still some weaknesses in the policy. In my view, the policy still very much treats algorithmic policing technologies as inevitable, as a net benefit so long as we can mitigate some of the risks. I think what you've been hearing from the witnesses today, including me, is that this is not the right framework from which to approach this technology, given the considerable harms that can be enacted through these technologies and the social context into which they're introduced.

One aspect of that policy process that was not formalized but that was discussed was the creation of an independent expert panel that includes expertise from a range of different areas, not simply technical expertise. That didn't come into fruition. There's still some conversation around that. I do think that's a step that could also be helpful at the federal level, to provide some kind of additional guidance and governance around not just facial recognition but all forms of algorithmic policing technologies.

Mr. Parm Bains: I'm also in British Columbia, so my questions are coming to you from Richmond, B.C. I want to know if there is anything in British Columbia that you've looked at and studied with the law enforcement agencies in B.C.

Ms. Kristen Thomasen: Well, I would flag that the Vancouver police force uses algorithmic policing technologies and would stand to benefit from looking at some of the processes that the Toronto Police Services Board has engaged in. To engage in that process on a federal and provincial level would be much more helpful, I think, than simply on a city or municipal police force level, because TPSB actually recognizes the—

The Chair: Ms. Thomasen, I'm sorry. I'm going to have to move to the next round.

Ms. Kristen Thomasen: No problem. I'll happily provide some submissions.

● (1250)

The Chair: Thank you very much.

We'll now go to Monsieur Villemure.

[*Translation*]

Mr. René Villemure: How much time do I have left, Mr. Chair?

[*English*]

The Chair: You have two and a half minutes.

[*Translation*]

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

Ms. Brandusescu, I'll turn to you again.

When you first spoke, you mentioned the Palantir company. I don't know if my colleagues know this, but on social media, Palantir presents itself as a very nice company and gives itself a very positive image.

At the same time, we know that projects like Gotham and Apollo are war projects, in a way. Palantir is a company that basically serves the military sector; it uses military technology to observe society. I therefore conclude that the words “ethics” and “Palantir” shouldn't be used in the same sentence.

I'd like you to clarify your thoughts on Palantir. I'd also like you to provide us with a list of the 105 companies you mentioned a little earlier and tell us what we should focus on to better understand the problem.

For now, I'll let you talk about Palantir.

[*English*]

Ms. Ana Brandusescu: Thank you for the question, and I'll gladly answer. I love that you stated that “ethics” and “Palantir” are not synonyms, because that is correct.

As I already stated, Palantir is a tech data analytics company, and hence this is the problem with the way “AI” is defined by the federal government. The definition is really broad, and I think it's just important for me to note what it is in this meeting. The Treasury Board defines “artificial intelligence” as “Information technology”—which is IT—“that performs tasks that would ordinarily require biological brain power to accomplish, such as making sense of spoken language, learning behaviours or solving problems.”

This is how Palantir managed to be on this list, which I will gladly share with you. The problem with Palantir is that it's actually really loved by governments all around the world, but it is getting some pushback right now from the EU—although it is involved in GAIA-X's project.

They were largely funded and created by Peter Thiel and others, and there are many conflict of interest cases even within that governance.

The problem is that they're still there. Clearview AI is also still there, although Canada has made a direct statement within OPC around having them out of the country, so to speak, although that's questionable. They're still scraping the web.

With Palantir, they really do data governance around the world. Why they are dangerous is that even though everyone knows they're not ethical and some people think they're cool, they're still hired by the law enforcement and—

The Chair: Thank you, Ms. Brandusescu. I'm going to have to go Mr. Green. We went a little bit over time there, but that's excellent information.

We move on now to Mr. Green for two and a half minutes.

Mr. Matthew Green: Thank you, Mr. Chair. My last set of questions will be directed through you to Ms. Molnar, who referenced what I suggest are the dystopian prospects of ”robodogs” and drones increasingly being utilized alongside AI and facial recognition at border crossings.

Can you explain how the existing power imbalances between the state and people crossing borders, especially refugees, can be further exploited by the use of AI and facial recognition?

Dr. Petra Molnar: Thank you so much. Ultimately, it comes down to the power imbalances, like you say, in this context. We already are dealing with an opaque and discretionary decision-making system in which, when humans are making really complex decisions, oftentimes it's really difficult to know why particular decisions are rendered and what we can do if mistakes are made. Now, imagine that we start augmenting or replacing human decision-makers with automated decision-making and increasing surveillance. It basically just muddies the already very discretionary space of immigration and refugee processing and decision-making.

Again, it's all along historical lines of power and privilege, and oftentimes, again, we're talking about communities that already have less access to justice and an inability, for example, to challenge mistakes that have really far-reaching implications.

Mr. Matthew Green: I want to get a bit more specific. In your report, “Bots at the Gate”, you state:

> For persons in need of protection under section 97(1) of the Immigration and Refugee Protection Act, error or bias in determining their application may expose them to the threat of torture, cruel and inhumane treatment or punishment, or a risk to their life.

Do we have a legal or moral obligation to ensure that a refugee process prioritizes the safety and security of the individual, and remove any technology or practices that increase the risk of error?

● (1255)

Dr. Petra Molnar: Yes, absolutely. When we're talking about refugee determination in particular, we're talking about an extremely high-risk application of technology. Like you rightly say, and like our report did in 2018, if mistakes are made and if someone is, for example, wrongfully deported to a country that they're fleeing from, the ramifications can be quite dire.

It's very concerning that we are testing and experimenting in this opaque and discretionary space without the appropriate oversights and safeguards. That is something that has to change, because it has real impacts on real people's lives.

The Chair: Thank you very much.

With that, we're going to get to the final two rounds.

We have Mr. Bezan for four minutes, and then we'll go to Ms. Hepfner and Ms. Khalid.

Go ahead, Mr. Bezan.

Mr. James Bezan: Thank you, Mr. Chair.

I thank our witnesses very much.

I'm going to direct my questions towards Ms. Brandusescu. You're well written. I perused at least three reports that you've already published, everything from “AI for the Rest of Us” and “Weak privacy, weak procurement: The state of facial recognition in Canada” to “Artificial intelligence policy and funding in Canada: Public investments, private interests”. I believe what you're suggesting is follow the money and you can see where the private interests lie.

Should federal and provincial governments be funding this type of AI technology and facial recognition technology?

Ms. Ana Brandusescu: I have a brief question back to you. When you say “be funding this type of technology”, should governments fund FRT?

Mr. James Bezan: That's what I'm asking you.

Ms. Ana Brandusescu: Okay. No, they shouldn't.

We're at this point where we're funding a lot of R and D, and some of the R and D can come up as FRT. Again, the end goal should be a ban.

We're already seeing the European Parliament calling for a ban on this. It is the latest ban that was called. It is possible to move from a moratorium to a ban, and we should. We're not even at a moratorium. We can start with law enforcement, but as other witnesses have mentioned, FRT is a problem across the government. It's not only a law enforcement problem, although law enforcement is the worse problem that FRT [*Inaudible—Editor*].

Governments should not fund it. They should fund civil society, digital rights groups and community groups that are doing this work to showcase all the harm that comes out of FRT. They know the social issues and the communities they work in. They are the experts and they should also be involved in the conversation of what the government decides to fund.

Mr. James Bezan: How do we look at both the policy directives and the funding of artificial intelligence and FRT? What do we then need to do on the side of privacy legislation, whether it's the Privacy Act or PIPEDA? What safeguards do we have to build in there to ensure that biometric data is protected?

Ms. Ana Brandusescu: That is a lot of questions. I'll take up one, which is we should turn the directive on automated decision-making—

Mr. James Bezan: You can send it in as well. You could also reply in writing after the committee winds up, but if you can give us a quick synopsis, that would be great.

Ms. Ana Brandusescu: Yes. A quick one would be to improve the directive on automated decision-making. Make sure that the internal reviews that are written every six months actually make it to the public. We're still waiting for the one that was supposed to be released last year. Apparently, it will be released in April. We're still waiting on it.

Others have mentioned how we shouldn't rely on investigative journalists to keep doing the work. The public should have this information. We should have updates. We should have home pages on the OPC and Treasury Board websites and in other spaces to show the latest involvement, like the procurement use of these technologies, like FRT, until they are banned.

The directive itself needs improvement. I will have those improvements and recommendations in writing later. We should follow the EU and the U.S. in putting together an act that covers the transparency of law enforcement, which is currently not covered by other public AI registries around the world. I will also put that in writing.

● (1300)

Mr. James Bezan: Would bringing in that accountability or the control powers leveraged by policing agencies across this country require amendments to our Criminal Code? How do we then tie that in with the private sector that's—

The Chair: I'm sorry, Mr. Bezan. You've only left enough time for a yes or no to that question. Then we'll have to move on.

Ms. Ana Brandusescu: I'll just give a maybe. That's not my expertise.

The Chair: Okay. Thank you.

With that, we'll finish it off with Ms. Khalid for four minutes.

Ms. Iqra Khalid: Thank you very much, Mr. Chair, and thank you to the witnesses.

I'll start with Ms. Molnar.

The United States put out a commitment that by 2023, 97% of all the people who travel through their airports will go through a facial recognition kind of system. In Canada, our IRCC immigration application assessment processes—not just for refugees, but also for all visitors and immigrants who are seeking immigration to Canada—are now being transitioned into an AI model of assessing the applications.

Can you perhaps talk a little bit about profiling and how this could directly or indirectly impact how institutional discrimination could occur?

Dr. Petra Molnar: What might be instructive is a comparator between what Canada could be doing and what the European Union is looking at under its proposed regulation on artificial intelligence. There, it clearly recognizes that individual risk assessments for the purposes of immigration and refugee processing are high risk. There are conversations around an outright ban of individualized risk assessment that can be used for profiling and for strengthening systemic discrimination, which is already something our immigration system is replete with.

I think there is an opportunity for the Canadian government to really think through how best to regulate the use of facial recognition technology for the purposes of immigration. You're absolutely right. It is already in use, both within Canada and also with its regional partners, like the United States, with whom it also shares a lot of the data.

Data sharing is an element we didn't really discuss today, but it's something that we all need to pay more attention to.

Ms. Iqra Khalid: Thank you.

Ms. Brandusescu, do you want to comment on that as well?

Ms. Ana Brandusescu: Yes, I agree with Ms. Molnar completely.

Ms. Iqra Khalid: Great. Thank you.

Lastly, we've heard some of the pros of facial recognition in locating missing children and in breaking up child pornography rings, for example. We do give up a little bit of our privacy to ensure the security and well-being of our communities.

Where does the commercial aspect of it fall in? Do any of you want to comment on that?

Dr. Petra Molnar: Perhaps I'll reiterate that when we're talking about commercial interests and the kind of bottom-line thinking that the private sector often brings into the mix, it's a very different framework for responsibility when it comes to the high-risk use of technology, particularly at the border, or as you're referencing, with human trafficking.

Again, we need to pay careful attention to the particular actors involved in the ecosystem in which these technologies develop and are deployed. None of this is neutral. It is all a political exercise.

Ms. Kristen Thomasen: I can also jump in.

I think in approaching thinking about regulation and limits on facial surveillance through the lens of regulating use, users or the designer availability of the technology, we can start to think about things like restraints or restrictions on the use of commercial facial surveillance systems. Instead, fund or develop in-house systems using data that is not just legally sourced, but sourced through fully informed consent and processes that ensure the dignity of the individuals whose data is being processed. It would be designed and used only for very specific use cases, as opposed to commercial systems like Clearview AI, for instance, that's being used in a wide range of different scenarios, none of which are taking into account the specific social context and implications for the people whose data is being processed or who are being affected by the use of that system.

I think there are ways we can really distinguish very narrow use cases and not build into a narrative that says we need facial recognition because it can be used to protect people from potential harm.

● (1305)

The Chair: Thank you so much.

That concludes the round.

With that, I thank our witnesses so much. We had some very important and interesting testimony today, so thank you to all of you.

The meeting is adjourned.

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

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

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