HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

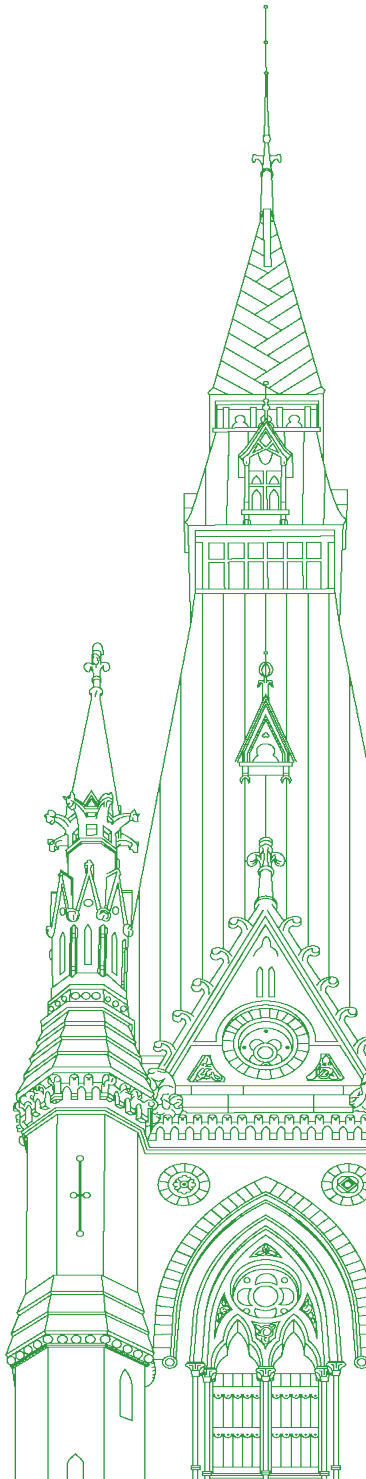
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 027

Thursday, June 16, 2022



Chair: Mr. Pat Kelly

Standing Committee on Access to Information, Privacy and Ethics

Thursday, June 16, 2022

● (1545)

[*English*]

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

Welcome to meeting number 27 of the House of Commons Standing Committee on Access to Information, Privacy and Ethics. Pursuant to Standing Order 108(3)(h) and the motion adopted by the committee on Monday, December 13, 2021, the committee is resuming its study of the use and impact of facial recognition technology.

I would like to now welcome our witnesses.

From the American Civil Liberties Union, we have Esha Bhandari. From the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, we have Tamir Israel, staff lawyer.

I apologize for the late start. It was just a function once again—and not uncommon at this time of the year—of the timing of votes in the House of Commons. The meeting was scheduled for one hour, from 3:30 to 4:30. We will still go ahead for the full hour, starting now.

With that, I will ask Ms. Bhandari to begin.

You have the floor for up to five minutes.

Ms. Esha Bhandari (Deputy Director, American Civil Liberties Union): Thank you very much, Mr. Chair.

Thank you to the committee for the invitation.

My name is Esha Bhandari, and I am a deputy director of the American Civil Liberties Union's speech, privacy and technology project based in New York. I am originally from Saint John, New Brunswick.

I'd like to speak to the committee about the dangers of biometric identifiers with a specific focus on facial recognition.

Because biometric identifiers are personally identifying and generally immutable, biometric technologies—including face recognition—pose severe threats to civil rights and civil liberties by enabling privacy violations, including the loss of anonymity in contexts where people have traditionally expected it, enabling persistent tracking of movement and activity, and identity theft.

Additionally, flaws in the use or operation of biometric technologies can lead to significant civil rights violations, including false arrests and denial of access to benefits, goods and services, as well as employment discrimination. All of these problems have been shown to disproportionately affect racialized communities.

What exactly are we talking about with biometrics?

Prior to the digital age, collection of limited biometrics like fingerprints was laborious and slow. Now we have the potential for near instantaneous collection of biometrics, including face prints. We have machine learning capabilities and digital age network technologies. All of these technological advances combined make the threat of biometric collection even greater than it was in the past.

Face recognition is, of course, an example of this, but I want to highlight that voice recognition, iris or retina scans, DNA collection, gait and keystroke recognition are also examples of biometric technology that have effects on civil liberties.

Facial recognition allows for instant identification at a distance without the knowledge or consent of the person being identified and tracked. Even in the past, identifiers that needed to be captured with the knowledge of the person, such as fingerprints, can now be collected without the knowledge of the person, which includes DNA that we shed as we go about our daily lives. Iris scans can be done remotely, and facial recognition and face prints can be collected remotely without the knowledge or consent of the person whose biometrics are being collected.

Facial recognition is particularly prone to the flaws of biometrics, which include design flaws, hardware limitations and other problems. Multiple studies have shown that face recognition algorithms have markedly higher misidentification rates for people of colour, including Black people, children and older adults. There are many reasons for this. I won't get into the specifics of that, but in part it's because of the datasets that are used but also flaws in real world conditions.

I also want to highlight that often the error rates that are shown in test conditions are exacerbated in real world conditions, which are often worse than test conditions—for example, when a facial recognition tool is being used on poor quality surveillance footage.

There are also other risks with face recognition technology when it is combined with other technology to infer emotion, cognitive state or intent. We see private companies increasingly promoting products that purport to detect emotion or affect, such as aggression detectors, based on facial tics or other movements that this technology picks up on.

Psychologists who study emotion agree that this project is built on faulty science because there is no universal relationship between emotional states and observable facial traits. Nonetheless, these video analytics are proliferating, claiming to detect suspicious behaviour or detect lies. When deployed in certain contexts, this can cause real harm, including employment discrimination if a private company is using these tools to analyze someone's face during an interview to infer emotion or truthfulness and deny jobs based on this technology.

I have been speaking, of course, about the flaws with the technology and the error rates that it has, which, again, disproportionately fall on certain marginalized communities, but there are, of course, problems even when the facial recognition technology functions and functions accurately.

The ability for law enforcement, for example, to systematically track people and their movements over time poses a threat to freedom and civil liberties. Sensitive movements can be identified, whether people are travelling to protests, to medical facilities or other sensitive locations. In recognition of these dangers from law enforcement use, at least 23 jurisdictions in the United States, from Boston to Minneapolis, and San Francisco and to Jackson, Mississippi, have enacted legislation halting law enforcement or government use of face recognition technology.

● (1550)

There's also, of course, the private sector use of this technology, which I just want to highlight. Again, you see trends now where, for example, landlords may be using facial recognition technology in buildings, which enables them to track their tenants' movements in and out of the building and also their guests—romantic partners and others—who come in and out of the building. We also see this use in private shopping malls and in other contexts as well—

The Chair: Ms. Bhandari, I'm sorry to have to interrupt you, but I will ask you to wrap up in the next couple of seconds so that we can carry on. You are a bit over time.

Ms. Esha Bhandari: Yes, absolutely.

I just want to conclude with a couple of policy recommendations.

One, government use of facial recognition technology should be prohibited—law enforcement use—but at the very least, there has to be regulation to constrain its use and protect individuals from the harm that can result.

Also, that same regulation should extend to private entities that use facial recognition technology.

Thank you very much.

The Chair: Thank you.

With that, we go to Mr. Israel for up to five minutes.

Mr. Tamir Israel (Staff Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic): Good afternoon, Mr. Chair and members of the committee.

My name is Tamir Israel and I'm a lawyer with the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic at the University of Ottawa, which sits on the traditional unceded territory of the Algonquin Anishinabe people.

I want to thank you for inviting me to participate in this important study into facial recognition systems.

As the committee has heard, facial recognition technology is versatile and poses an insidious threat to privacy and anonymity, while undermining substantive equality. It demands a societal response that's different and more proactive than that to other forms of surveillance technology.

Face recognition is currently distinguished by its ability to operate surreptitiously and at a distance. Preauthenticated image databases can also be compiled without participation by individuals, and this has made facial recognition the biometric of choice for achieving a range of tasks. In its current state of development, the technology is accurate enough to inspire confidence in its users but sufficiently error prone that mistakes will continue to occur with potentially devastating consequences.

We have long recognized, for example, that photo lineups can lead police to fixate erroneously on particular suspects. Automation bias compounds this problem exponentially. When officers using an application such as Clearview AI or searching a mug shot database are presented with an algorithmically generated gallery of 25 potential suspects matching a grainy image taken from a CCTV camera, the tendency is to defer to the technology and to presume the right person has been found. Simply including human supervision will, therefore, never be sufficient to fully mitigate the harms of this technology.

Of course, racial bias remains a significant problem for facial recognition systems as well. Even for top-rated algorithms, false matches can be 20 times higher for Black women, 50 times higher for native American men, and 120 times higher for native American women than they are for white men.

This persistent racial bias can render even mundane uses of facial recognition deeply problematic. For example, a United Kingdom government website relies on face detection to vet passport image quality, providing an efficient mechanism for online passport renewals. However, the face detection algorithm often fails for people of colour and this circumstance alienates individuals who are already marginalized by locking them out of conveniences available to others.

As my friend Ms. Bhandari mentioned, even when facial recognition is cured of its biases and errors, the technology remains deeply problematic. Facial recognition systems use deeply sensitive biometric information and provide a powerful identification capability that we know from other investigative tools such as street checks will be used disproportionately against indigenous, Black and other marginalized communities.

So far, facial recognition systems can be and have been used by Canadian police on an arrested suspect's mobile device, on a device's photo album, on CCTV footage in the general vicinity of crimes and on surveillance photos taken by police in public spaces.

At our borders, facial recognition is at the heart of an effort to build sophisticated digital identities. “Your face will be your passport” is becoming an all-too-common refrain. Technology also provides a means of linking these sophisticated identities and other digital profiles to individuals, driving an unprecedented level of automation.

At all stages, transparency is an issue, as government agencies in particular are able to adopt and repurpose facial recognition systems surreptitiously, relying on dubious lawful authorities and without any advance public licence.

We join many of our colleagues in calling for a moratorium on public safety and national security related uses of facial recognition and on new uses at our borders. Absent a moratorium, we would recommend amending the Criminal Code to limit law enforcement use to investigations of serious crimes and in the absence of reasonable grounds to believe. A permanent ban on the use of automated, live biometric recognition by police in public spaces would also be beneficial, and we would also recommend exploring a broader prohibition on the adoption of new facial recognition capabilities by federal bodies absent some sort of explicit legislative or regulatory approval.

Substantial reform of our two core federal privacy laws is also required. Bill C-27 was tabled this morning and it would enact the artificial intelligence and data act, as well as reform our private sector law, our federal law PIPEDA. Those reforms are pending and will be discussed, but beyond the amendments in Bill C-27, both PIPEDA and the Privacy Act need to be amended so that biometric information is explicitly encoded as sensitive, requires greater protection in all contexts and, under PIPEDA, requires express consent in all contexts.

● (1555)

Both PIPEDA and the Privacy Act should also be amended to legally require companies and government agencies to file impact assessments with the Privacy Commissioner prior to adopting intrusive technologies. Finally, the commissioner should be empowered to interrogate intrusive technologies through a public regulatory process and to put in place usage limitations or even moratoria where necessary.

Those are my opening remarks. I thank the committee for its time. I look forward to your questions.

The Chair: Thank you.

For the first round of up to six minutes, we have Mr. Kurek.

Mr. Damien Kurek (Battle River—Crowfoot, CPC): Thank you very much. I'd like to thank our witnesses for joining us here today. As I often start, please feel free to follow up with specific recommendations. Certainly, that is valuable when it comes time for this committee to put together its report.

I appreciate the content of your opening statements. One big challenge that I think lawmakers and public policy-makers have in terms of addressing this issue is trying to find that right balance. There's law enforcement that says it needs every tool available to help fight crime, to help protect victims, etc. On the other side we have the valid argument that we need to ensure that vulnerable people, groups, are protected and that the rights of Canadians, in the case of Canada, are respected.

I'd ask this question to both of you. Do you have any recommendations for this committee as to how to find that right balance? I'll start with Mr. Israel.

Mr. Tamir Israel: When you're talking about an intrusive technology like this, the onus is on the government to make its case for the use of the technology. One big problem—and I know the committee has heard this—is that currently adoption happens at the ground level, and any legislative response comes in response to that.

Some of our recommendations would flip that around by either creating a legislative obligation to go to the legislature and make the case for the use of some of these techniques in advance, or alternatively, by empowering the regulator, the independent Privacy Commissioner of Canada, to play a proactive role in assessing and approving or disapproving elements of these technologies. I think that might be one meta consideration for how to address some of these challenges more broadly.

Mr. Damien Kurek: Thank you.

Ms. Bhandari.

Ms. Esha Bhandari: Just to follow up on Mr. Israel, I would say I agree that, when we're talking about a new technology, particularly one with as many flaws as facial recognition, the onus has to be on law enforcement. In this case we know the flaws. Multiple studies have shown the disproportionate error rates and the consequential impacts on people's lives. There have been a few high-profile instances in the United States of Black men being falsely arrested by facial recognition match and the devastating consequences for people because of that.

At the very least, do extensive study to show that those flaws and error rates have been eliminated and that there aren't disproportionate impacts on people based on demographics. That's just not there now. In the absence of that, essentially the widespread use of facial recognition technology in these specific contexts is running an experiment on the population at large.

We're not there yet, but certainly, looking forward I'd also agree that the concerns about persistent tracking and identity theft, all of those exist. Any balance that this committee strikes in its recommendations has to take into account the harms that will result even if the technology functions as it's claimed to function.

● (1600)

Mr. Damien Kurek: Thank you for that.

As a little bit of a follow-up on that, Ms. Bhandari, this committee had studied the usage of mobility data in terms of Canada's public health response to COVID-19. It was interesting. During your opening statement I heard some consistency in the remarks you shared to some of the concerns that this committee heard over the course of that previous study. I'm wondering if you have any observations, if you had a chance at all to see the work that this committee did. Was there anything you'd like to add to that?

Ms. Esha Bhandari: There's definitely, I think, a tie-in to those concerns, because location tracking is one of the harms from even properly functioning facial recognition. It's a society in which every move we make is in a database to be used. I think the concerns about mobile tracking and contact tracing, when they come without those safeguards, are the same for facial recognition.

Again, we don't currently live in a society where we expect, regardless of whether we're out in public or not, our every move would be accessible to government, to law enforcement and to private companies, potentially, that want to market to us or exploit us in some way. The technology is there to track us everywhere we go all day long.

Location tracking concerns that this committee considered previously are also applicable here.

Mr. Damien Kurek: I appreciate that.

I have one final question in my last minute.

We often hear the example of Clearview AI and how that is no longer used in Canada—no longer contracted by law enforcement. However, there certainly are a whole host of other providers, and some further applications that may not have as direct a purpose as Clearview AI.

Could you perhaps share with the committee your experience with other providers or other example that this committee should maybe be aware of?

There are about 30 seconds left.

Ms. Esha Bhandari: There are certainly other providers.

The American Civil Liberties Union has settled with Clearview in the United States to limit them from selling their database to private entities in the United States. However, that is one company among many companies.

Many of the companies are not necessarily consumer facing. They won't be the big tech names that people are aware of. Again, transparency is so key. The public may not know of these companies in the way that they know of big social media, for example.

Mr. Damien Kurek: Thank you.

The Chair: Next we'll go to Ms. Saks, for up to six minutes.

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

Thank you to the witnesses here today. I'll start with you, Mr. Israel, if I may.

In September 2020, the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic released a report on facial recognition, which you wrote. It focuses primarily on its use at borders.

In a very specific fashion, because of time, what were the main findings of the report? Could you give the top three? Then I have a follow-up question.

Mr. Tamir Israel: I would say the main findings were that facial recognition is being adopted at the border without due consideration for the harms it would cause, without much external oversight and often without regard to existing policies, such as the Treasury Board's policy on artificial intelligence, where you are supposed to bring in external guidance when adopting intrusive technologies like that.

Then, once it is adopted, it often gets repurposed very quickly for reasons beyond the narrow reasons of the context in which it was developed.

The last one is that it often provides a link between digital and physical presences in ways that allow for automation in the application of many other automated assessment tools, which is problematic in and of itself.

Ms. Ya'ara Saks: Thank you.

You said in your opening remarks that human interaction with these platforms is insufficient. We've heard from other witnesses that human interaction is actually an imperative part of being able to utilize this technology.

Could you clarify that a little bit, please?

Mr. Tamir Israel: I agree that it's an integral part, but it is important to also recognize that it is not enough.

I think this committee heard, as well, from a witness on how humans interact with facial images that they are presented with, and how their own biases creep in. The example provided was of a photo lineup that is often used by police, and how it replicates the type of image output that you often get from a facial recognition system, where it gives you maybe the top 10 or 15 matches. We know that, as an investigative tool, that has led to a lot of problems in the past for police.

That is the type of human supervision that we're talking about. It's worse in the context of facial recognition systems, because the tendency is to trust in the automated results of the system and that they produced an accurate match. You're questioning it even less than in the context where you get just a general photo lineup and try to figure out who a person is. What it ends up doing is embedding cognitive and other biases.

● (1605)

Ms. Ya'ara Saks: I understand. There is an element of human error in everything in life.

However, my next question on that is this. If we move to a legislative guardrail on this, can you actually legislate for human error? We can legislate for human intervention, but how do we legislate for human error, then? The train has left the station on these technologies, and we're trying to look at what the guardrails would be. Can we really legislate human error?

Mr. Tamir Israel: I think legislating a human in the decision-making loop is an important thing to include. I think it's also important to recognize that it doesn't solve all of the problems. It's often presented as the solution, but you're often going to have a lot of bias problems, even with a human involved in the investigation. Beyond that, you still need more.

We still recommend a moratoria, given the wide potential for harm with this particular technology, until we get to a better and more concrete regulatory and technologically developed state.

Ms. Ya'ara Saks: Thank you so much.

I'm going to move to Ms. Bhandari, if I may.

I'd like to touch on something that, unfortunately, we didn't get to enough in this study, which is location tracking technologies used in commercial and retail spaces. For example, Cadillac Fairview is a big mall owner here in Canada. They tend to have cameras and other technologies in their spaces, from what I understand.

We talk a lot about the legislation in terms of the relationship of private companies with law enforcement. I'll start with you, Ms. Bhandari, and perhaps also Mr. Israel.

What are your thoughts on how we legislate that private or commercial relationship with these types of technologies going forward, in an ideal world, if there was a moratorium and we had time to think about this?

The Chair: Ms. Bhandari, before you respond to Ms. Saks' question, I would ask you to move the boom of your microphone up a little bit. We had a little bit of trouble with your audio.

Let's go ahead and I'll stop you again if we need another adjustment.

Ms. Esha Bhandari: I hope this is better.

To address the question on private sector use, the harms are real. I'll highlight a few examples.

In Michigan, for example, a skating rink was using a facial recognition tool on customers who were coming in and out. A 14-year-old Black girl was ejected from the skating rink after the face recognition system incorrectly matched her to a photo of someone who was suspected of previously disrupting the rink's business.

We've seen private businesses use this type of technology, whether it's in concert venues, stadiums or sports venues, to identify people on a blacklist—customers they don't want to allow back in for whatever reason. Again, the risk of error and dignitary harms involved with that, the denial of service, is very real. There's also the fact that this tracking information is now potentially in the hands of private companies that may have widely varying security practices.

We've also seen examples of security breaches, where large facial recognition databases held by government or private companies have been revealed in public. Because these face prints are immutable—it's not like a credit card number, which you can change—once your biometrics are out there and potentially used for identity purposes, that's a risk.

Similarly, we've seen some companies—for example, Walgreens in the United States—now deploying face recognition technology that can pick out a customer's age and gender and show them tailored ads or other products. This is also an invasive practice that could lead to concerns about shoppers and consumers being steered to discounts or products based on gender stereotypes, which can further segregate our society.

Even more consequentially, it's used by employers—

● (1610)

The Chair: I'm sorry to have to do it again, but we are a fair bit over time on this round.

I'm going to go next to Monsieur Villemure for six minutes.

[*Translation*]

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

Good afternoon, Ms. Bhandari.

This committee has heard about all sorts of horror—and error—stories. We heard about prejudice that was directed primarily at racialized populations, for example. Your association is an advocacy association, so it is militant.

I will, for a moment, play devil's advocate.

Is there any advantage to using facial recognition?

[*English*]

Ms. Esha Bhandari: Thank you for your question.

I agree with what Mr. Israel said earlier, which was that the onus and the burden should be on the entities seeking to use facial recognition. Certainly I think private companies would say there's an advantage. They are making money off of it. Collecting data, as we know, is very profitable. I don't think that's an advantage this committee should consider when weighed against the invasion of rights.

When we're talking about law enforcement and government uses, I think it's true that new technology will always be claimed to be solving age-old problems, but I don't see any evidence that the use of facial recognition technology and any perceived benefits it might bring to law enforcement outweigh the type of transformation it would render in society.

[*Translation*]

Mr. René Villemure: In your view, the infringement of rights is so great that it is not worth talking about the advantages, which are often commercial—which, by the way, is not the purpose of our study.

Is this right?

[*English*]

Ms. Esha Bhandari: Yes.

[*Translation*]

M. René Villemure: You mentioned motion detectors earlier. In the past, I've read some studies about this, some of which were a bit frivolous. They were talking about the ability to recognize people's sexual or political preferences through facial recognition.

Is any of this possible? Are these claims, on the contrary, totally fanciful?

[*English*]

Ms. Esha Bhandari: There are a lot of companies marketing the ability to do this right now. The science is not there to support it.

Currently, all the experts say that there is not a reliable link between our physical or biological manifestations and those mental states or propensities, but I think the real fear, of course, is that society will come to accept these links, that we'll go back to an age where we thought physiognomy or physical characteristics revealed character and that this new technology will be seen as providing new and objective truth.

I'm not sure that the fear is that it will in fact reveal mental states, but the concern is that it is being marketed as such.

[*Translation*]

Mr. René Villemure: I'm coming back to your last comment.

Should the public get used to electronic surveillance? Isn't it a waste of time to try to legislate the use of billions of images that are already circulating?

[*English*]

Ms. Esha Bhandari: It is absolutely not a lost cause, and there is plenty of time for the government to take action. Regulating the flow of information going forward is critical to putting a halt to some of the harms we've seen.

It's not inevitable that we continue to be awash in biometric information, that we continue to be tracked. What has come before, of course, has come before, but moving forward, we can put guardrails in place. We can have strong laws and regulations. Just because an industry has been unregulated in the past doesn't mean that it's too late to solve it now.

[*Translation*]

Mr. René Villemure: You talk about user-provided content. Shouldn't we be raising awareness about privacy or the risks related to the use that is made of data?

[*English*]

Ms. Esha Bhandari: That is certainly one element of it. I also want to highlight, though, that oftentimes data is collected from people without their consent. So many people who use the Internet to shop or to search for information don't know how they're being tracked.

As I mentioned, face prints being captured are often captured without our consent. Nobody meaningfully can say “no” if surveillance cameras are gathering that. This is not a problem of people willingly giving up their biometrics. Most of the time, people don't know, which is why a knowledge and consent requirement before biometrics are captured is very critical.

[*Translation*]

Mr. René Villemure: Could you briefly tell us about the lawsuit you launched against Clearview AI in the State of Illinois?

● (1615)

[*English*]

Ms. Esha Bhandari: Yes. We filed a lawsuit against Clearview under an Illinois state law known as BIPA, the Biometric Information Privacy Act, and we settled that lawsuit.

Under the terms of the settlement, there are two key provisions. Clearview can no longer provide to any private entity access to its database containing millions and millions of face prints nationwide—permanently. It's a permanent ban on selling to private entities in the country, with a few exceptions, and a five-year ban on law enforcement access within Illinois.

The only way we were able to bring this lawsuit is that Illinois has the Biometric Information Privacy Act, which makes it rare in the United States, and that law shows the potential of regulation. That law is what enabled us to sue Clearview and reach the settlement whereby Clearview can no longer sell its face print technology to private entities around the country.

[*Translation*]

Mr. René Villemure: I would ask you to send us documentation on the law in question or the lawsuit you have filed, if possible. It would be helpful to us.

[*English*]

Ms. Esha Bhandari: I would be happy to do that.

[*Translation*]

Mr. René Villemure: Can you tell me if Clearview AI can still sell its technology outside of the United States at this time?

[*English*]

Ms. Esha Bhandari: Our lawsuit doesn't address anything they do outside the United States. That's correct.

[*Translation*]

Mr. René Villemure: All right.

Thank you very much.

[*English*]

The Chair: Next will be Mr. Green for up to six minutes.

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

I'd like to pick up on that. I can recall coming back through an international flight and being herded through an American Homeland Security checkpoint. I believe it was at Pearson. It was the first time that I was having to contemplate iris scans. I'm wondering if the witnesses can speak—and perhaps we can start with Ms. Bhandari—about the way in which Nexus in our airports has.... Has her work in the States led to any investigations or research on Nexus's public-private biodata collection service?

Ms. Esha Bhandari: One of the areas that we have been concerned about is the expansion of facial recognition and other biometric technology in airports. We haven't looked specifically at Nexus, but the same principle holds with, for example, the global entry system in the United States.

The concern, of course, is that as people become required to provide face prints or iris scans to access essential services—going to the airport, crossing the border, entering a government building—it facilitates a checkpoint society the likes of which we haven't seen before. These are not contexts in which people can meaningfully opt out, so one clear area of regulation could be providing people with a meaningful opt-out by saying that, if you don't want to prove your identity via an iris scan, we'll provide you the option to do so another way, with your passport, for example, or with your Nexus card, for example.

On the airport use and the border use, because it's such a coercive environment, because people don't have the choice to walk away, that has been a big concern.

Mr. Matthew Green: Go ahead, Mr. Israel.

Mr. Tamir Israel: It's exactly as Ms. Bhandari said. It's a big problem, because programs like Nexus are opt in, in a sense, but the pressure to get through the border—the explicit use of the border as a pain point to encourage travellers to sign up for these types of systems—is a problem.

Canada, for example, piloted a program with the Netherlands, one developed by the World Economic Forum. It's basically a digital identity, housed on your phone, with a lot of your passport information and additional social identity verification program information. The idea was to see if that could be used in replacement of a passport, in order to facilitate border crossings. Facial recognition was the technology built into that system. The end vision of that system—it's very explicit—is getting travellers to voluntarily sign up for it to avoid delays at the border, because it gives you access to faster security processing. However, it later becomes available to banks, telecommunication companies and other entities, as well, for similar identity verification programs.

Mr. Matthew Green: Oh boy, Mr. Israel, I think you might have touched the third rail when you talked about the World Economic Forum, in this context.

I have an interest in your report. You talked about how some evidence suggests that Canadian border control agencies appear to be unaware of racial biases inherent in these systems. What little public information is available suggests these capabilities may have been assessed for general levels of inaccuracy but not for racial bias. I'll reference the ongoing saga of the no-fly lists for kids. In this country, we literally have children being flagged, identified and put on no-fly lists because they might have Muslim-sounding names. They are caught up in some kind of bureaucratic nightmare, quite frankly, when trying to travel.

Can you talk about the risks posed by that lack of awareness about racial bias, particularly in terms of having human guardrails in place to help offset some of these inconsistencies and inaccuracies?

● (1620)

Mr. Tamir Israel: That's certainly a very valid and salient concern.

The no-fly lists have been a long-standing problem. There have been proposals to create facial recognition-enabled lists with comparable objectives. CBSA did, in fact, pilot one for a while, and decided not to implement it yet, I think. That is something they piloted, and that's deeply problematic.

The response from CBSA has been concerning. For example, one CBC report tried to probe into the racial biases in one of those facial recognition systems. When they asked for more detailed breakdowns of error rates and racial bias rates.... First, through access to information requests, it appeared that CBSA was not aware, at the time of its adoption, that these were real. Later on, they responded that there are national security concerns with providing this type of error data, which is just not.... In other jurisdictions, this is publicly available. It's required to be publicly available by law in other jurisdictions. That's not a good approach.

More recently, there have been developments, in the sense that CBSA announced they will try to implement a biometric study hub within their infrastructure, but we haven't seen much going on yet.

Mr. Matthew Green: Quickly, before my round wraps up....

I think about the nightmare that is Toronto Pearson—the three- to four-hour-long waits for domestic travel, because security lanes are closed. Do you think these are the right preconditions for filtering people into things like Nexus?

I know when I'm standing in line and look at the business class, visa or Nexus lines, they are empty. Do you think the inconsistencies and inefficiencies at our borders might result in a peak of people applying for things like Nexus?

Mr. Tamir Israel: I think it really is putting people in an unfair position of having to choose that, if it's the only way they can make their airport and travel experiences a little less unpleasant.

The direction things are going in is worse. There are proposals around the world to automate that screening process. You'll walk up to a screen and get a facial recognition scan. There will be an assessment of your profile pulled in digitally, and you'll automatically get channelled through gates to a high-security, medium-security or low-security line.

That will just be this on steroids. If you don't have the right profile in place to interact with this—

Mr. Matthew Green: Yes, I can imagine where this is headed. I've been pulled out into secondary more than my fair share of times.

Thank you very much, Mr. Chair.

Thank you very much to our witnesses.

The Chair: Thank you. We went quite a bit over time, but I let it go. We were getting good information. Hopefully, we'll try to keep our rounds tight to time.

With that, next we have Mr. Bragdon. Welcome to our committee. You have up to five minutes.

Mr. Richard Bragdon (Tobique—Mactaquac, CPC): Thank you, Mr. Chair.

Greetings to all the other committee members here today.

It's a very important subject we're covering. A lot of Canadians have genuine and sincere concerns when they consider this. As our world continues to change at such a rapid pace and we're seeing concerns about privacy continue to rise—balanced with the need for security for populations—I think Canadians want to be assured that all the possible safeguards are put in to protect individual rights and the privacy rights of Canadians.

Mr. Israel, I'll go to you first. Your report makes several interesting recommendations when it comes to what you would like to see in a legislative framework for facial recognition technology, which we do not currently have. In your report, you write that the need for legislative backing applies to border control implementations that rely on a form of consent, such as opt out or opt in.

Do you believe all use of facial recognition technology by border control should have an opt-in, opt-out component?

● (1625)

Mr. Tamir Israel: Yes. Part of the problem with the technology is that, if there's not an explicit opt-in requirement, you're not even necessarily aware that you're being subjected to the technology. For example, with the customs screening mechanisms they have at Pearson, from the traveller's experience, you don't necessarily realize that a facial recognition scan is happening. There is no explicit obligation to get your consent. That's equally problematic. In the U.S., we saw examples where there was an obligation to provide an opt-out, but the signs were hidden in the corner. People didn't see them very well.

I would say that requiring, at the very least, an opt-out with very clear notification, and perhaps even an opt-in, would be a useful addition.

Mr. Richard Bragdon: Can you further explain the difference between centralized and decentralized architecture in facial recognition technology? How is each type of system susceptible to breaches? What breaches might they be susceptible to? Can you explain that for us a bit?

Mr. Tamir Israel: In a centralized system, all the images are held in one spot. If I were to walk up to a camera, my picture would be taken and it would be compared to the centralized database of millions and millions of images.

A decentralized system would be something like what we have on our passports, where there's a digital passport image encoded on the passport. When I use that, a picture is taken. The digital image on my passport gets compared with the one that was just taken. The comparison happens in that way.

There are still security risks, because the security on the digital radio device encoded on the passport can have breaches, but then you breach one passport. Not all of the biometric templates are in one place, where it's a lot easier to just grab the entire database.

Mr. Richard Bragdon: Further to this, images of travellers who are children or elderly are less accurately identified by FRT, in addition to people of ethnic backgrounds. That's a significantly large group of people combined.

For this reason, should all travellers, once again, be able to opt in or opt out of the FRT systems to avoid being misidentified when travelling?

Mr. Tamir Israel: In many jurisdictions, at the airports, facial recognition is not applied to travellers under the age of 14 and over the age of 79, I believe. Again, that greatly undermines any efficiency gains you get from adopting these systems, while subjecting everybody else to the intrusiveness of having to give up their biometrics. I think that needs to be taken into account when assessing how effective this is.

It is also a safeguard that has to be in place and taken into account, so that these systems are not applied to those age groups where it's known that there are significant drop-offs in accuracy. For the rest, I think maybe an opt-in is okay, but I think a moratorium is still a good idea, given where things are in terms of the rapidness of the adoption of this technology and the ongoing errors that it produces.

Mr. Richard Bragdon: Following up on that, you're recommending that there be a moratorium until we know more. That would definitely seem to be a wise and prudent approach. A lot of this is emerging technology. The technology is coming in, and there's a lack of awareness in the Canadian population as a whole as to the ramifications of this type of technology and what it could mean for their privacy rights, their individual rights and where that information is going to be stored and where that information may get shared. I think there are a lot more questions to this than there are potential benefits, from what we're hearing.

Thank you.

The Chair: You're welcome, and you did use all of your time and then some, so there isn't time for a response.

We will go now to Mr. Bains for up to five minutes.

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

Thank you to our guests for joining us today. I'm going to ask a question of Mr. Israel.

One of the key findings of the report states that FRT has higher levels of social acceptance in comparison to other biometrics. What other biometric technologies is FRT being compared to, and why would FRT be more acceptable than the alternatives?

Mr. Tamir Israel: I think Ms. Bhandari touched on this as well.

Because facial recognition operates surreptitiously and doesn't have associations with things like fingerprinting that historically come out of a criminal justice kind of context, there's a bit less social stigma attached to it in the minds of people, although there shouldn't be, because it's increasingly used in the same context as mug shots, etc.

The other part of that is what Ms. Bhandari was talking about before, which is that, because it happens remotely and with less direct interference with individuals, sometimes people are just not aware of how intrusive FRT is in comparison to other biometrics, where you have to physically grab peoples' fingers or scan their eyes in a way where they're leaning in to ensure a good iris scan. For those two reasons, facial recognition has been easier to get adopted.

● (1630)

Mr. Parm Bains: My next question is this: How should FRTs be regulated in the private sector? This is for Mr. Israel again.

Mr. Tamir Israel: I think the harm in the private sector can be even worse in some contexts than in the public sector. There's probably wider variation.

We recommend empowering the Privacy Commissioner to look into the adoption of intrusive technologies and impose conditions and even moratoria on specific technologies as a meta way of addressing this. We also recommend encoding biometric information as sensitive and explicitly requiring express consent for biometric information as is, I believe, the case in the Illinois law Ms. Bhandari mentioned and in the Quebec law now.

I think those are two good steps and then perhaps even a moratorium. It's just a broader use case.

Mr. Parm Bains: Thank you.

Ms. Bhandari, U.S. police authorities have been much more willing to engage with FRT technology.... I'm sorry—wrong question.

The state of Illinois has a law that applies specifically to biometrics, the Biometric Information Privacy Act, and therefore to facial recognition technology. What are the benefits of this legislation?

Ms. Esha Bhandari: One of the main ones is that it enabled us to hold a company like Clearview accountable for creating a database of hundreds of millions of people's face prints without consent and selling it to private companies and law enforcement for a whole host of purposes.

We have been advocating for other states to adopt biometric privacy laws and, in particular, make changes, because the Illinois law is at this point quite old, and we have more knowledge about the technology and the risks of the technology.

Among the recommendations that we make in the context of states that were to adopt a legislation like the Illinois BIPA, one is clearly requiring companies to obtain notice and written consent before collecting, using or disclosing any person's identifier, and prohibiting companies from withholding services from people who choose not to consent, so that they're not given the choice of accessing a service versus not accessing the service if they're not willing to give up their biometrics.

We also urge that any legislation require businesses to delete biometric identifiers after one year of the individual's last interaction with a business. For example, if someone gave their biometrics to access a service and consented but no longer has a relationship with that business, the business shouldn't be able to hold on to and amass a database of these sensitive biometrics. As Mr. Israel mentioned, there's a risk of breach. We've seen instances of those, and there's no need for those private entities to hold on to those. We advocate adopting legislation like Illinois' BIPA but also updating it.

Mr. Parm Bains: Are there any modernized laws in other states that Canada could be inspired by?

Ms. Esha Bhandari: I would have to think and get back to the committee on whether there was sort of a perfect model. I think the Illinois law is a good place to start and I think that there have been proposals in places like Maryland and Maine. Those laws have not been enacted but they are out there. Those models are available and we urge their passage. I would look to Maryland and Maine specifically for models.

Mr. Parm Bains: Thank you.

How much time do I have, Mr. Chair?

The Chair: You're done. You had about three seconds left.

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

[*Translation*]

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

Ms. Bhandari, this morning, the Government of Canada introduced Bill C-27, which, among other things, implements the Digital Charter. Part 3 of the bill is entitled "Artificial Intelligence and Data Act."

The bill therefore deals with artificial intelligence and facial recognition. It will be sent to committee for study so that we can discuss it and make suggestions for improvement.

From what you know of the Biometric Information Privacy Act, or BIPA, what should we look to in that legislation to enrich our digital charter that will eventually be implemented?

● (1635)

[*English*]

Ms. Esha Bhandari: I will point out to the committee that the Maryland bill is SB 335, which is a biometric privacy law. I think that is one model this committee could look to.

[*Translation*]

Mr. René Villemure: I'm so sorry to interrupt you, but we have very little time.

Is there anything in the BIPA that Canada should take inspiration from?

[*English*]

Ms. Esha Bhandari: The consent provisions are key and it has to be meaningful consent. I think Mr. Israel spoke about the downsides of opt-out consent, and particularly one concern we have is that we all interact with so many businesses, particularly online, that if you have to opt out every time people get opt-out fatigue.

I think affirmative express consent is one thing that should inspire this committee and meaningful opt-in consent for particular uses.

[*Translation*]

Mr. René Villemure: Thank you very much.

Do you believe that one day we will be able, as European legislation now allows, to invoke the right to be forgotten, or the right to have our images removed from databases?

[*English*]

Ms. Esha Bhandari: Yes, that's a critical part of any regulation. There should be a sunset period, as I mentioned. We've suggested one year after the last interaction with a business as a default, but certainly any time an individual chooses to have their biometrics deleted from a database, that option should remain.

Again, recognizing that people may choose to use biometrics for a very specific purpose, even with the risks that entails, that doesn't give carte blanche to the company to hold on to those because they are such sensitive identifiers and could lead to identity theft and a whole host of other issues.

[*Translation*]

Mr. René Villemure: We will need to pass a law that will clearly give people the ability to have their images easily removed from databases.

Is that correct?

[*English*]

Ms. Esha Bhandari: Yes, and there should also be a clear limit on any private sector collection of biometrics. There should be a clear limit on sharing with other entities, including law enforcement, without the consent of the individual. We should carve a very important regulation so that it's not that once you give up your biometrics for one purpose it can be shared broadly.

[*Translation*]

Mr. René Villemure: Thank you very much.

[*English*]

The Chair: Thank you.

Now we'll go to Mr. Green for two and a half minutes.

Mr. Matthew Green: Thank you.

I'd love for the guests to be able to summarize in their final thoughts any information for the good and welfare of this committee for the consideration of our analysts when drafting a report.

I'll start with Ms. Bhandari.

Do you want to take a minute and perhaps share any concluding thoughts you might have that you want the committee to take away from this?

Ms. Esha Bhandari: My final thoughts are that I would urge the committee to act expeditiously. The technology's developing every year, and as things stand it's a too-far unregulated field that is inflicting harm every day. There are very concrete, specific laws that can be enacted. There is regulation that can be effective, regardless of what has happened before, so I hope that the committee will keep in mind the very specific recommendations that Mr. Israel provided and others. It's not too late to act.

Mr. Matthew Green: That's very important.

Mr. Israel, would you like to just conclude.

Mr. Tamir Israel: I would second what Ms. Bhandari is saying. It's not too late to act.

I would just also add really quickly that we have a very big enforcement problem in Canada. Obviously we had rulings against Clearview here as well. Clearview is currently challenging those rulings against it from the B.C. privacy commissioner, the Alberta privacy commissioner and the Quebec commissioner.

Federally though, it did not challenge the federal Privacy Commissioner's ruling because that ruling is not binding, so it's essentially, “take it as a recommendation and move on.” I think the enforcement mechanisms that will come through in the private right of action that is coming through Bill C-27—which I imagine may come before you shortly—is something that you would also like to take a look at very closely when you're considering how to make sure that whatever laws you put in place are respected by Clearview and all the other companies that follow its model.

Mr. Matthew Green: Thank you so much to both witnesses. I'm happy to end the rest of my time, Mr. Chair.

The Chair: Okay. That catches us up by about 45 seconds. Thank you, Mr. Green.

The final two rounds go to Mr. Kurek, and then we'll be done with Mr. Fergus.

Go ahead, Mr. Kurek.

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

Again, thank you to the witnesses.

Ms. Bhandari, you mentioned that there were a couple of exemptions to the Clearview biometrics. You had referenced this in one of your previous answers. Would you be able to expand on that for the committee?

● (1640)

Ms. Esha Bhandari: I'm sorry that I don't have the specifics of those exemptions to provide. They're written into the law for very specific purposes. I can send details to the clerk later on the specifics of the settlement, which outlines what those exemptions in BIPA are.

Mr. Damien Kurek: That would be appreciated.

Mr. Israel, you had referenced the WEF's known travel digital identity program. I've certainly heard from many constituents who are concerned about the idea of a very powerful type of digital ID. The government is participating in a pilot program in that regard. Do you have any concerns with the KTDI pilot program that you could outline to the committee, in particular if there's any concern about how a program like this may disproportionately affect certain elements of the population, whether they be people of colour, racial minorities, young, old, etc.?

Mr. Tamir Israel: Yes, absolutely.

I am very concerned. The pilot did get a little bit interrupted by the pandemic, and I don't know how aggressively it's being moved forward now. I'm very concerned with the idea of using the pinpoint of the travel experience to encourage people to opt in and create these types of profiles, knowing that they're then going to be used against them, not just in border control contexts, where many marginalized communities are already at a massive disadvantage, but here and abroad, in other countries that end up implementing the same system. It's intended to be a global system. It's also with the idea that these same systems are going to then be used by the private sector for fraud detection or identity management in interactions with private companies.

The facial recognition component of this is a big part. All the errors there are going to, again, fall most heavily on visible minorities and members of marginalized communities. Then the other assessment and social ranking mechanisms that are included in this identity verification program that will sit on your device and be linked to through your facial recognition also tend to weigh very heavily and disproportionately against members of marginalized communities.

I think this is not the way to go, personally.

Mr. Damien Kurek: I appreciate that. If you'd bear with me here, certainly I've heard from constituents who are concerned about the inclusion of one's political beliefs as to whether or not they could travel, the inclusion of something like race as to whether or not they're allowed to rent an apartment, or a whole host of hypotheticals that could be included in some nebulous database that exists somewhere on a server that may or may not have human oversight. Certainly I think we all need to be very careful about that. Is that something you would agree with?

Mr. Tamir Israel: Absolutely. Part of the challenge with this type of system is that, by relying on artificial intelligence assessing tools, you're able to implicitly do what you couldn't do directly. You couldn't necessarily say, "I'm not renting to you because you're indigenous," but then maybe you could adopt an algorithm that relies on biased historical data and ends up coming to that conclusion without the transparency that would let someone challenge that type of decision explicitly. That's a very big problem as we move towards this broader set of assessment mechanisms. Again, facial recognition is a tool that really allows a lot of implementation of those types of mechanisms. The KTDI profile has lots of elements of that built into it.

Mr. Damien Kurek: Just in my few seconds left, you had referenced the public sector and private sector. I know that Air Canada, KLM and some airports that are quasi private-public entities, depending on where they are in the world, are some of the partners included in this program. Is that of concern to you?

Mr. Tamir Israel: Absolutely. That's a concern more broadly with facial recognition systems. There's a lot of back and forth in other jurisdictions—and we anticipate it will get here eventually—where airlines are incentivized to adopt facial recognition systems for border control reasons. They're even given some funding sometimes and then they use that for their own commercial reasons.

There's a lot of really problematic interplay between how the private sector is increasingly picking up a lot of this very sensitive data at the borders.

The Chair: Thank you, Mr. Israel.

For the last five minutes, we have Mr. Fergus.

● (1645)

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

Through you, I'd like to really thank these two witnesses. They've been outstanding and I really do appreciate their insights.

For the two witnesses, if you don't know how committees work here in the House of Commons, we actually have to receive written or verbal testimony for us to make recommendations. We have to hear something on the issue before we can go forward on it.

I would like to take this on a different tack. I'll ask both witnesses this today.

Mr. Israel, in response to Mr. Kurek, you were talking about transparency—or the other side, the opacity—of these FRT systems and how they surreptitiously take pictures and identify people. I guess my question would be this: Are either of you aware of a registry of companies that engage in facial recognition technology? Is there a list somewhere of companies, governments or agencies of governments that engage in capturing images for the purposes of FRT?

Mr. Tamir Israel: I'm not aware of a list.

Sometimes you get lists when there's a procurement process. Often you get a number of companies that register to sign up for that, but that takes a little bit of investigative work from journalists to really uncover that and it's never complete.

I will say really briefly that some states—and Ms. Bhandari may or may not know more about this—do actually require data brokers to register. That might be something to look at in connection to these types of companies if we want to get more transparency on exactly what is happening on the ground.

Hon. Greg Fergus: Ms. Bhandari.

Ms. Esha Bhandari: I'm also not aware of any centralized registry.

I will note that in the United States, the National Institute of Standards and Technology did a study on facial recognition tools a couple of years ago. It was a widely publicized study that found the racial bias inaccuracy. In that study, I believe they looked at least 99 commercial facial recognition tools that were sold by companies. That didn't even include any facial recognition tools from big companies like Apple, Amazon or Facebook.

That's just to give you a sense of the number, but I am not aware of any centralized registry.

Hon. Greg Fergus: The next question would be for both of you.

Should there be such a registry for transparency purposes?

Ms. Bhandari, let's start with you.

Ms. Esha Bhandari: I certainly think that is an important first step, particularly for enforcement authorities to know who they regulate, just as in other industries. If you regulate banks, usually the banks are not operating in secret so that you wouldn't know they're subject to these regulations.

As Mr. Israel mentioned, there is a movement of having data brokers register, but it wouldn't necessarily capture companies that sell facial recognition or other algorithmic tools. Requiring that kind of transparency on a product that you sell would allow for a private right of action, private enforcement of violations of laws or regulation, or for regulators to know who to be monitoring.

Hon. Greg Fergus: Mr. Israel.

Mr. Tamir Israel: Yes, precisely. I think that's correct. I think Ms. Bhandari is right that the database list would not capture these types of tools. Perhaps it could be a model to build on.

I would also suggest that, in the European regime, some types of more intrusive techniques require a privacy impact assessment be filed with the data protection regulator early on in the process. Something along those lines might help. It wouldn't necessarily capture small and early-onset tools or all the tools, but it might be another way of getting a window into what's developing earlier on.

Hon. Greg Fergus: Let me see if I can just get in one more question in the minute that's left to me.

In the European context, with their digital protections, or perhaps in any state or subnational organization, are you aware of whether they have a requirement for companies to declare publicly that they are employing this technology?

I'm not just talking about people who sell the service. I'm talking about companies that might use it only for their own purposes.

Ms. Esha Bhandari: There have been some proposed laws in the United States that would require the disclosure of algorithmic tools or automated decision-making, and I think facial recognition technology would be included in that.

Some laws that we have seen enacted at the city or state level require transparency for government use. For example, if law enforcement is adopting new technology like facial recognition, that transparency is mandated so that there can be democratic community oversight. In many cases, city councils didn't know what their police departments were using and what technology they had. These laws would mandate that it be made public, and then the city councils and other democratic bodies could exercise oversight.

I've seen it in the government use context.

● (1650)

The Chair: Thank you very much.

Mr. Tamir Israel: I think that addition would be great in the Canadian context, as well. Also requiring that type of notice would be very—

The Chair: We're significantly over time. My microphone wasn't activated, but I was in the midst of wrapping things up.

Thank you very much to both of our witnesses for their testimony. We got great information today. Thank you very much for that.

With that, the meeting is adjourned.