CANADIAN CIVIL LIBERTIES ASSOCIATION
ASSOCIATION CANADIENNE DES LIBERTES CIVILES

INCLO
INTERNATIONAL NETWORK OF CIVIL LIBERTIES ORGANIZATIONS

TORONTO, CANADA. MARCH 8, 2023

Faces under surveillance:

Global perspectives on FRT use and regulation

Moderator: Brenda McPhail

Panel: Ben Wizner, lawyer and Director of the Speech, Privacy, and Technology Project at the American Civil Liberties Union (ACLU) in the US; **Gil Gan-Mor**, lawyer and Director of the Civil and Social Rights Units at the Association for Civil Rights in Israel (ACRI); **Emmanuelle Andrews**, Policy and Campaigns Manager, Liberty, UK; **Manuel Tufró**, Director of Violence and Security at Centro de Estudios Legales y Sociales (CELS) in Argentina.

Brenda McPhail: "Turning to today's topic: facial recognition. Facial recognition is a type of biometric technology that uses artificial intelligence to identify individuals through their facial features. It works by creating templates, kind of maps, of key facial features that allow comparisons between live and stored biometric templates. You can think of it like a facial fingerprint. It's an identifier that's based on your body, that is unique to you.

Facial recognition is a type of biometric technology that uses artificial intelligence to identify individuals through their facial features. It works by creating templates, kind of maps, of key facial features that allow comparisons between live and stored biometric templates. You can think of it like a facial fingerprint. It's an identifier that's based on your body, that is unique to you.

"Here in Canada, we lack adequate legislation to fully protect our faces or, more broadly, any highly sensitive personal biometric information. That's something that emerged very clearly during a recent scandal here which was duplicated in some of the other countries represented here today when police forces were revealed to be using a facial recognition tool produced by a company called Clearview AI, a tool which was very definitively declared, by our Privacy Commissioner here in Canada, as illegal.

"CCLA, the Canadian Civil Liberties Association, has been working very actively to advocate for the kind of regulatory protections that we so clearly lack because we see the very real risks to rights and freedoms that this technology raises not just to our privacy but to those rights that privacy supports and enables, including equality rights, particularly with this technology known to be less accurate on faces that are black or brown or female or young. In other words, any faces other than those that are white and male.

It affects our rights to freedom of expression and association because those rights are chilled or thwarted when state bodies can not just watch us as we go about our daily business, but identify us; pin us to a time and place.

"It affects our rights to freedom of expression and association because those rights are chilled or thwarted when state bodies can not just watch us as we go about our daily business, but identify us; pin us to a time and place.

"So today we are so grateful to be able to draw on the expertise and the experiences of a truly exciting panel, representing four of our INCLO partners, in order to learn from them and help us, as a civil liberties organization in Canada, and perhaps you individuals, participants in the audience, think through the implications of this technology and the actions that we might take, alone or together. So, joining me today, in alphabetical order but not seating order: Emmanuelle Andrews, here to my immediate left, who is the Policy and Campaigns Manager at Liberty in the United Kingdom; to her left, we have Gil Gan-Mor who is a lawyer and Director of the Civil and Social Rights Unit at the Association for Civil Rights in Israel. At the far end, we have Manuel Tufró, Director of Violence and Security Group and I'm going to absolutely butcher this name in Spanish but, in honor of Manuel who has agreed to do this panel in English, not his first language, I'm going to make a valiant attempt, the Centro de Estudios Legales y Sociales, or CELS. And to my immediate right, Ben Wizner, lawyer and Director of the Speech, Privacy, and Technology Project at the American Civil Liberties Union.

"As we turn now to our panel conversation, I would like to remind our audience that you are welcome to ask questions in the Q&A interface that's a part of your webinar screen, as they arise. We will spend some time at the end of our session answering those questions. But you don't have to wait for the end of our conversation to put them in the queue. We

also want to let you know, as a group that's sensitive to issues of privacy and surveillance, that this webinar is being recorded so please take that into account when you're considering the kind of information that you choose to share in those Q&A fields.

"To start the conversation, I'm going to turn to my right, to Ben, and ask him to kick off the conversation, by telling me about a key project or an initiative, or a legal case that you're working on that has to do with Facial Recognition Technology."

Ben Wizner: "Thanks Brenda and thanks to everyone for joining this webinar. Before I get to the specific case, I want to say that the technology already exists to end public anonymity. Imagine walking through city streets and being stopped every 100 meters by a police checkpoint and having to turn over your identification. The infrastructure for making this with cameras with facial recognition linked to databases of our identities already exists and the only thing preventing that kind of digital checkpoint society from being created is law and policy and the work that we'll do to prevent that kind of dystopian picture from becoming the reality.

Imagine walking through city streets and being stopped every 100 meters by a police checkpoint and having to turn over your identification. The infrastructure for making this with cameras with facial recognition linked to databases of our identities already exists and the only thing preventing that kind of digital checkpoint society from being created is law and policy and the work that we'll do to prevent that kind of dystopian picture from becoming the reality.

"I think there's really, in a way, two major problems with facial technology that I think are somewhat in tension with each other and I'm going to mention both and then talk about a case. The first is that, as you said, in your lead-in, this is a technology that has had a disparate impact, in particular racially disparate impact, in that it has been proven to be less accurate for faces that are outside the dominant minority of the training sets, meaning white and male. That has led, in the US, to cases of mistaken arrests where people were actually handcuffed in front of their children and taken off to jail because of a mistake with facial recognition. We represent a black man in Michigan named Robert Williams who had this occur. And a lot of work needs to be done to highlight these cases,

to address these kinds of inequalities and I think, really, to make people understand the harms that these technologies can create.

"But I wouldn't want us to focus solely on the ineffectiveness of facial recognition because I can tell you that these companies have been working day and night to fix them, and are getting better, and better and better at identifying all kinds of faces that some of us, as offended and disgusted as we are at the racial inequalities that the technology has created, are at least as worried about what's going to happen once those problems have been fixed. And once we have a technology that is accurate, more than 99% of the time, and identifying us, and we'll talk about the Clearview AI case a little bit later on, but that is a company that essentially respects no boundaries, and is essentially trying to make the norm the kind of surveillance activities that larger companies have been too nervous about doing.

"We didn't need Clearview AI to create this capability of letting every police officer identify every face. Facebook and Google could have done this ten years ago but they didn't because they were worried about public backlash. We now have small companies that are emerging that don't have the same commitments to customers; aren't as worried about regulators; and are really pushing the boundaries here to move closer to the world that I described in my introduction."

But I wouldn't want us to focus solely on the ineffectiveness of facial recognition because I can tell you that these companies have been working day and night to fix them, and are getting better, and better and better at identifying all kinds of faces that some of us, as offended and disgusted as we are at the racial inequalities that the technology has created, are at least as worried about what's going to happen once those problems have been fixed.

Brenda McPhail: "Thanks Ben. Actually, I'm going to ask you now to pass the mic down to Manuel and if you'd like to make a bit of an opening statement or start talking about one of your key projects or initiatives."

Manuel Tufró: "OK, thank you very much, Brenda. Hi everyone. First of all I'd like to thank the CCLA for the invitation. As Brenda said, English is not my first, or even my second, language. So maybe at some point, I won't be as fluent or maybe I'll go back to my notes, I hope you will excuse me. As Brenda said, I'm part of a human rights organization

in Argentina, we work with a very broad agenda, maybe too broad but security policies have been a key issue for us for a couple of decades and that's how we came across facial recognition technology which is what we are going to discuss today.

"I'd like to make a brief comment on terminology, even if English is not my first language. When we did the translation to Spanish, of INCLO's report on FRT, *Stories From Around the World*, we decided to talk about facial recognition systems and not technologies because we all understand that technology per se means software, algorithms, search engines, they are key components of broader systems or arrangements of political and bureaucratic practices and regulations and pre-existing databases in which these technologies are embedded.

"I am highlighting this because in Argentina, many of the problems we detected are not really hardcore technology problems, but rather problems in other parts of these complex systems or arrangements. Of course this doesn't mean that the technology doesn't have problems but we don't know which problems those are, because in Argentina we can't access information about the technology. We don't know which software the government is using, at least at the local level. And even in the context of a lawsuit, that I will comment on today, the authorities would not give us detailed information about the technology they are using. So we are talking about facial recognition systems to highlight this problem.

"We've been working since 2019 in litigation against the implementation of facial recognition systems in Buenos Aires city. We've been carrying this case, together with a sort of hacker organization called ODIA which means 'hate' in Spanish and also stands for the *Argentine Computer Law Observatory [Observatorio de Derecho Informático Argentino]*. And we started this litigation focusing on the general problems that research on FRT around the world has repeatedly pointed out, such as the risks of mistakes and wrongful identification, racial and ethnic biases, etc.

...many of the problems we detected are not really hardcore technology problems, but rather problems in other parts of these complex systems or arrangements. Of course this doesn't mean that the technology doesn't have problems but we don't know which problems those are, because in Argentina we can't access information about the technology.

"But as the judge gathered more information it was clear that the oversight and the accountability systems regarding this facial recognition system were non-existent. So last year, in September, the judge ruled that the facial recognition system, in Buenos Aires city, is unconstitutional and it was suspended, and the judge said that it had been implemented without complying with the legal provisions for the protection of the constitutional rights of the inhabitants of the city.

"So the decision, which is a good decision for us, is not centered on facial recognition technology, but on the fact that it was prematurely implemented and deployed in what I would call careless conditions regarding the respect to individual rights. So the local government appealed this decision and now we are awaiting the decision of the High Court of Justice of Buenos Aires city. *[Since this webinar, the Appeals Court of the City of Buenos Aires (Cámara de Apelaciones en lo Contencioso Administrativo y Tributario) confirmed the decision by the local judge that the implementation of the Facial Recognition System employed by the Government of the City (Sistema de Reconocimiento Facial de Prófugos) was unconstitutional, because of the lack of, or serious deficiencies in, legally required oversight mechanisms that aim to protect the constitutional rights of the citizens of Buenos Aires, such as the right to privacy or freedom of movement.]*

...as the judge gathered more information it was clear that the oversight and the accountability systems regarding this facial recognition system were non-existent. So last year, in September, the judge ruled that the facial recognition system, in Buenos Aires city, is unconstitutional and it was suspended...

"This is a moment of a bit of tension in our organization, the tension between lawyers and researchers. I don't know if you're familiar with this in your own organizations, I'm exaggerating a bit, but lawyers are saying now, 'we won this case, the judge ruled in our favor, so we don't need to go deeper about knowing about this technology. That could even be counterproductive for the litigation strategy.' But we want to know more about this software. We want to know which software it is, how it works, because this judicial decision leaves the door open. It says that with an adequate oversight system, facial recognition technology could be used again. So that is a discussion we are having now in our organization.

"We also know, on another level, that the federal government has a software called Luna. I don't know if anyone has heard about it? We know they are using it for criminal investigations and not, as far as we

know, for surveillance. But we couldn't gather more information about it either. So I will leave it here now."

Brenda McPhail: "And I think that's a really good transition to have Emmanuelle next because Liberty, the organization she belongs to, conducted I think the very first litigation challenging facial recognition. There's some commonalities there with the situation Manuel is describing, so Emmanuelle - I've got a Manuel/Emmanuelle sandwich here and I'm trying to be very careful to pronounce the first syllables! Emmanuelle, if you'd like to make a bit of an opening statement and tell us about a project or initiative that maybe you're working on."

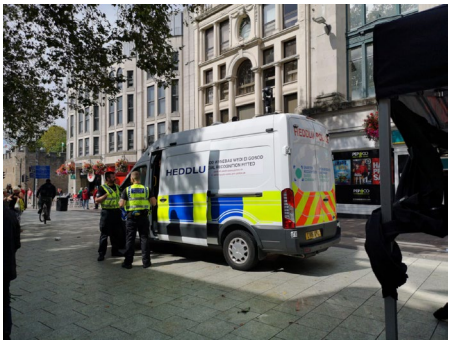
Emmanuelle Andrews: "Thank you, Brenda and thanks everyone for having me. I will talk about the legal challenge that Liberty won back in 2020. But I'll save that for some of the other questions I think. So, just to start, I wanted to give a quick overview of the landscape of facial recognition in the UK at the moment. It's being deployed and used in a vast array of different contexts and situations, from supermarkets using it to enforce blacklists on individuals entering their stores. Schools have come under fire for deploying it against children purchasing lunch. We've seen the adoption of search identification tools which one developer boasted on their website was offering a dangerous superpower from the world of science fiction [PimEyes] which could not be closer to the truth. And, of course, police use. So, from the potential use of live facial recognition with body-worn cameras to retrospective facial recognition, which essentially turns every photo or video into a possible surveillance tool, as well as operator-initiated facial recognition, so police officers using a mobile phone app with facial recognition embedded to facial recognition watches that are used to monitor individuals subject to immigration control.

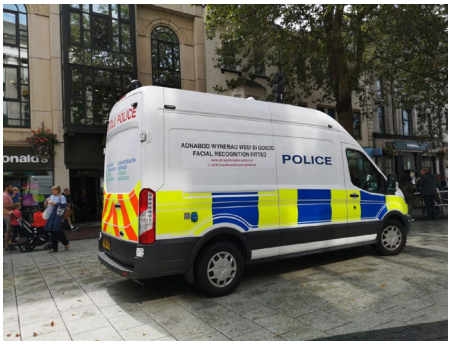
[FRT is] being deployed and used in a vast array of different contexts and situations [in the UK], from supermarkets using it to enforce blacklists on individuals entering their stores. Schools have come under fire for deploying it against children purchasing lunch.

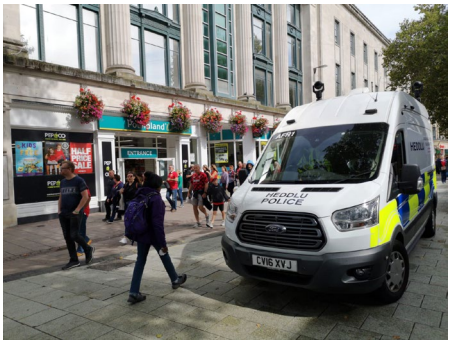
"So there's so many different ways in which institutions beyond the police are using it. I think Liberty's main concern at the moment is police use and that's definitely our main focus. And we're particularly concerned about police use of facial recognition at protests. We were talking earlier in the day about the raft of new protest legislation that's been passed or due to

be passed at the moment [in the UK]. And included in that legislation is a massive expansion of the potential for people to be criminalized for things they wouldn't have previously been criminalized for, including the use of new civil orders that have criminalizing penalties if you breach any of the conditions attached to them. And a good example, a good kind of reference point for this, is the use of football banning orders. So banning particular people from football matches. And we know that the police are using it and have used it at football matches to certainly capture whether people are breaching these orders. So we wouldn't be surprised if police – if they're not already using it to capture people at protests and

[...] looking at different ways we can oppose this technology, and more creative ways, is becoming especially more urgent.







A POLICE LIVE FACIAL RECOGNITION SURVEILLANCE VEHICLE IN CARDIFF CITY CENTRE, WALES. PHOTOS: LIBERTY

to surveil protestors and activists and advocates and particularly, given the increasing raft of new oppressive legislation against protest, against our ability to protest – use that as an opportunity to expand the context within which they're using it. And the UK has a really dark history when it comes to covert human intelligence, using spies to integrate into political activism and social justice movements. So that is a particularly concerning area that we're focusing on at the moment.

"I mentioned the case that Liberty led back in 2020, and that was also a protest case. Ed Bridges, the claimant, had been protesting outside an arms fair and it was in that case that the Court of Appeal ruled South Wales police use of facial recognition unlawful which I will talk about more in a little while.

"But I was also going to say that, in addition to the kind of threats to protest and our concerns around facial recognition use at protest, to be a bit positive, we have just seen a local council in London pass a moratorium on facial recognition which is fantastic. It was literally a month, a couple of months ago. And this was the borough of Newham which was a) one of the first places that facial recognition was ever trialed in London and in the UK and b) it's one of the most ethnically diverse places in London. So, on the one hand, the fact it was deployed in a predominantly black area raises alarm bells about it being deployed against marginalised communities, and the ways in which police will use technology to oppress black communities in particular. But it is also incredible that the local council did pass a moratorium banning it. So I think that also, and I'm sure we'll talk about it later as well, but there are so many different routes for us to affect change in this area. And I think one of those routes for us will be increasingly looking at local routes. Because, as I'm

sure many people know, our government is increasingly authoritarian and our opposition party provides less comfort. I'm trying to be really diplomatic, but yes, our current government is really authoritarian and our opposition party, to be frank, is little better. So I think, looking at different ways we can oppose this technology, and more creative ways, is becoming especially more urgent."

Brenda McPhail: "That was a really great list, expanded list, of terrifying ways this technology can be used. Do you have anything to add, Gil?"

Gil Gan-Mor: "Yes, I think so. Hi everybody. You know, usually when we are talking about these technologies or systems of facial recognition, we try to distinguish between democracies and countries that are not democracies. The Association for Civil Rights in Israel has the privilege of having both. And one context is that our work, within Israel, which is, you can say, a democracy - we are struggling with that at the moment - but it's still a democracy. We have a constitutional right to privacy and if the police or another law enforcement agency wants to use facial recognition, there are a lot of limits about it: it has to be in accordance with a specific law, it needs to be proportional, and so on. Therefore, we were, until now, able to stop the police from using facial recognition. But we also have, in our backyard, the Occupied Palestinian Territory which is a territory that is occupied by Israelis for more than 50 years and Palestinians who are living there are living under the Israeli military regime and under occupation and this is not a democracy. This is a wholly different environment, different legal environment, where there are no norms that we usually recognise in a democracy. There is no right of privacy that is being enforced in any way, and therefore this is an excellent kind of lab for the authorities to try new surveillance technologies.

And one of these facial recognition technologies is called the Blue Wolf

[The Occupied Palestinian Territory] is a wholly different environment, different legal environment, where there are no norms that we usually recognise in a democracy. There is no right of privacy that is being enforced in any way, and therefore this is an excellent kind of lab for the authorities to try new surveillance technologies.

system. It was never introduced officially, by anyone. We just found out about it from talking to people on the ground, from evidence of ex-soldiers that were asked to use this system, evidence that was collected by our

colleagues in Breaking the Silence which is an organization of ex-soldiers that are trying to fight occupation. The system works in a way that the soldiers are requested by the army to collect as many photos, identified photos, of Palestinians, of any age, children, men, women, elderly. These photos are taken and put into a photo bank of all the Palestinians. It started in one city, in Hebron, and now they are expanding it across the entire West Bank. Then they put a lot of cameras that can recognise a person based on their biometric facial data and they use the cameras to just identify people in public spaces and walking near checkpoints, or at any place where they want, to just have a temporary checkpoint.

The soldiers have a cellular app and this app tells the soldier if the person

The [FRT] system works in a way that the soldiers are requested by the army to collect as many photos, identified photos, of Palestinians, of any age, children, men, women, elderly. These photos are taken and put into a photo bank of all the Palestinians. It started in one city, in Hebron, and now they are expanding it across the entire West Bank. Then they put a lot of cameras that can recognise a person based on their biometric facial data and they use the cameras to just identify people in public spaces and walking near checkpoints, or at any place where they want, to just have a temporary checkpoint.

is either 'green', 'orange' or 'red'. Green means they were identified as 'OK', can go and aren't needed for anything; orange means that this person is needed for more questioning and they can detain the person until they get further orders; and red means that this person needs to be arrested and taken to the police or to the army.

"We are now looking into this system and the way it's being used in the West Bank. I think this is a kind of frightening mirror and reflects the reality of what will be when these systems will be a part of our lives. The army is actually using Orwellian language and say that, 'no this system is not against the population, it's for the population; it's going to help the population because if you are recognised, and you are 'green', you are free to go. So, actually, we are trying to help innocent people.' But obviously, if we are talking about Palestinians in the Occupied Territory, many of them are labeled as a 'risk' - so many people, even if they have a family tie with someone who is under investigation or anything like that. Another thing that is alarming is that it has a very serious chilling effect on the

lives of Palestinians who, already before this technology, were under a lot of surveillance and pressure from the army.

"Just one example, the army is using people that they know are 'in the closet', members of the LGBTQ community that are 'in the closet', to force them to co-operate and give them information. So just imagine where someone is going to a place which is known for being a place for LGBTQ community meetings and there is facial recognition camera at that place, recognising all the people that are going there. This is a serious threat for their freedom and ability to exist in this area. I hope I depressed you enough!"

Brenda McPhail: "Rather than depressed, I think we can all be warned. Here, in Canada, we sometimes think that it can't happen here. One of the things that we can draw from these examples, is that across a wide range of countries, with a wide range of types of government, inevitably, whenever this technology comes into play, the same kinds of risks run as a common thread, regardless of jurisdiction. So, I mean, here in Canada, I mentioned that we found out that Clearview AI was being used by police and the fact of that relationship highlighted that we have gaps in our laws when it comes to regulating this technology so my next question for the panel is: have you had a similar experience? Either with Clearview itself, with another specific product? How did you find that your laws did, or did not, stand up to the test of regulating that invasive surveillance? And I'm going to start with Manuel this time."

Manuel Tufro: "When the facial recognition system was approved in 2019 in Buenos Aires city, it was presented as a tool for searching for fugitives and people with arrest orders, through the use of CCTV cameras in public spaces. And the ministerial order that created this system also ordered the creation of a special, legislative commission for oversight. Of course, this was nothing but a formal concession I would say and the commission never existed. The facial recognition system

When the FRT system was approved in 2019 in Buenos Aires city, it was presented as a tool for searching for fugitives and people with arrest orders... it was intended to work by processing data between a database of fugitives and wanted people which consisted maybe of 30,000 to 40,000 names...but it turned out the government sought consultations about more than 7 million people, not those 30,000 or 40,000 fugitives.

was implemented with what I would call automatic consensus, much like what happened with CCTV in previous decades. And the legal framework was truly never intended to regulate its use. In fact that was the ground for the judicial decision to suspend the facial recognition system. So the question is in this absence of oversight, what happened with the practices of security forces?

"Well, facial recognition was intended to work by processing data between a database of fugitives and wanted people which consisted maybe of 30,000 to 40,000 names, and the biometric data gathered by the national identity database in Argentina. But when the judge asked this national identity database how many individual consultations were received from the Buenos Aires government, it turned out that the government sought consultations about more than 7 million people, not those 30,000 or 40,000 fugitives. So, clearly, Buenos Aires police and maybe other offices were accessing that biometric data for other purposes, entirely different to searching for fugitives. And to this day, we don't know exactly how and why they accessed the data of about 7 million people. So, long story short: no, the legal framework didn't stand up to the test. But, then again, it wasn't a properly legal framework but rather like a blank check of the implementation of FRS [Facial Recognition Systems]."

Buenos Aires police and maybe other offices were accessing that biometric data for other purposes, entirely different to searching for fugitives. And to this day, we don't know exactly how and why they accessed the data of about 7 million people.

Brenda McPhail: "Ben?"

Ben Wizner: "I realize we both mentioned Clearview AI and we may not have adequately explained what that company is and what it does. Clearview AI is a facial recognition start-up that scraped the internet for billions and billions of photographs. These are photographs that people had posted to social media sites and even though those social media sites say, 'you're not supposed to come on our sites and scrape them for photographs, they didn't take a lot of steps to prevent a company, like Clearview, from doing that. And then Clearview developed a sophisticated facial recognition algorithm that allowed their customers who are principally police organizations to submit to Clearview any kind of photo. It could be a still photo, from a surveillance camera, basically any photo, and then have Clearview return to them dozens, hundreds of photos of that person that identified the person because they also

scraped all of the information from these public social media sites. So, what it essentially meant was that if you give this company a photo of anybody who's watching this right now, they're going to be able to say, with a very, very high degree of accuracy who you are and also link to other information of yours.

"Now, we didn't know that this company existed. And this is the real legal challenge. The way we found out this company existed is that an anti-surveillance advocate in Chicago was doing Public Record Act requests and an Illinois police agency accidentally sent him a legal memo that had been prepared by a very prominent American lawyer, explaining why everything that Clearview AI did was legal and protected by the [US] Constitution. He had never heard of the company, was stunned by what he read, gave that memo to a reporter from the New York Times who then spent the better part of a year figuring out for the rest of us what this company was up to. And their business model essentially was to make Clearview AI available to lots of individual police officers all around the United States without even telling their superiors, without going through any kind of procurement process at all but put it into the hands of police so that they could be dazzled by how effective it was and then advocate to their bosses, to retain Clearview and to give them money. It wasn't originally only intended for police officers. They hoped that private companies would be able to use this. They were handing out the app to some of their investors. One of their billionaire investors used the app to identify the man that his daughter was bringing around and get background information about them! So this really was, you know, a way to end privacy as we know it. And only because of this mistake, it had come to light in a way that allowed us, in the US, to bring a

[...] their business model essentially was to make Clearview AI available to lots of individual police officers all around the United States without even telling their superiors, without going through any kind of procurement process at all but put it into the hands of police so that they could be dazzled by how effective it was and then advocate to their bosses, to retain Clearview and to give them money. It wasn't originally only intended for police officers. They hoped that private companies would be able to use this. They were handing out the app to some of their investors. One of their billionaire investors used the app to identify the man that his daughter was bringing around and get background information about them.

legal challenge. And then there have been other legal challenges around the world.

"This is something I want to highlight here, which is that, at least in the United States, typically, law enforcement agencies are already using surveillance technology for years before we have the chance to actually challenge it, legally. So they're not waiting for legislation to say: you're now authorized to use facial recognition. They use facial recognition until either a legislature or a court tells them they can't. And they've been very clever about how they use it, particularly in criminal cases. So if they were presenting the results of facial recognition algorithm tests in court routinely, we have an opportunity to come at it and to do discovery and to find out how it's being used. But instead they usually use facial recognition to identify their suspect and then find other information before they go to a court for a warrant and we never see any mention in a criminal trial that facial recognition was used at all. It all happened in the early investigatory stages and it doesn't turn up in any way that would allow us to see if there are constitutional limitations in how it can be used in criminal cases.

The real, darkest scenario is something that looks a lot like the way it would be used in Western China where the entire infrastructure of CCTV cameras now has this kind of identifying technology that can be used in real-time.

"And I'll just add that, and I think that this is probably happening in some of our societies, one of the debates among privacy advocates is, you know, is it time now for us to go into legislatures and parliaments and legislate all of the possible restrictions and use cases or do we still have a chance, as we heard occurred in London and has happened in a few cities in the US, to get communities to ban law enforcement use of this technology. I would say we're seeing both approaches in the United States. But I think everyone recognizes that, before long, we're going to have to engage in a debate that distinguishes different kinds of uses of facial recognition.

"The real, darkest scenario is something that looks a lot like the way it would be used in Western China where the entire infrastructure of CCTV cameras now has this kind of identifying technology that can be used in real-time. We know that, in the United States, these capabilities are being investigated by law enforcement and intelligence agencies but

have not been rolled out in that sense. And then there are other kinds of uses of facial recognition technology that bother us a lot but where we think that with some kind of warrant requirements, with some kinds of restraints on how the information can be used, that would be better than what we have now which is essentially, we don't know, we don't know what the cops are doing."

Brenda McPhail: "That's all ringing true in the Canadian context where we are now seeing facial recognition technology appear in cases, as part of disclosure before lower courts to be mentioned in judgments and that's something that CCLA is looking at - can we find those cases? Can we identify how courts are dealing with this technology? As a sort of precursor to thinking through, you know, is there an opportunity to litigate and how can that also feed into our policy work. But I also think it's fascinating that you identify, you know, the concerns across a spectrum of uses. We've heard about a spectrum of uses already this evening because we're having those same conversations here in Canada, in part, due to the backlash against the Clearview case, we now have police forces in Canada saying, 'well so, we'll just go back to the uncontroversial use of facial recognition where we check photos from crime scenes against our own mugshot databases'. And what that sort of characterisation of that use of facial recognition technology, as uncontroversial, does, is skip over the entire legacy of systemic racism that lies beneath who gets surveilled, who gets arrested, who gets charged in our societies, which, here in Toronto, Canada, we have very good data to suggest, are predominantly people who are black, and people who are indigenous, and people who are homeless. So we know that even in what a rhetorically uncontroversial use, according to our law enforcement agencies, there are fundamental problems in the ways that the datasets have been created that render even that kind of use deeply problematic, which feels like a good transition

[...] we now have police forces in Canada saying, 'well so, we'll just go back to the uncontroversial use of facial recognition where we check photos from crime scenes against our own mugshot databases'. And what that sort of characterisation of that use of facial recognition technology, as uncontroversial, does, is skip over the entire legacy of systemic racism that lies beneath who gets surveilled, who gets arrested, who gets charged in our societies, which, here in Toronto, Canada, we have very good data to suggest, are predominantly people who are black, and people who are indigenous, and people who are homeless.

to go back to Emmanuelle. And if you could tell us one of the cases, or whether or not, as you work through this, if you've found that the laws you have in place are successful or unsuccessful in dealing with that wide spectrum of risks that you identified."

Emmanuelle Andrews: "Yes, definitely, so, just to quickly pick up on the Clearview AI situation. We also have been, Clearview AI in the UK has also been the subject of intense scrutiny for the exact same reasons. And the Information Commissioner's Office, so our kind of data protection ombudsman, in the UK, fined Clearview AI for what it was doing, so scraping the internet and passing that information on to police forces. And just to give an example of the ways in which these start-ups work, they are really insidious. For example, in the UK, we know they will go to police force fairs and literally hand out the technology for free and say, 'oh, just trial this'. The way that they're promoting their technology is very intense.

[...] to answer the question of what kind of laws or policies we have to facilitate or limit police use of facial recognition, the Clearview AI example is a good example of, right now, we have good data protection laws, but that is subject to change. We've got more legislation going through at the moment that might really restrict the Information Commissioner Office's powers and role so there's no saying that if this situation were to happen again, we would have the same kind of enforcement mechanism and hefty fines imposed on Clearview.

"But to answer the question of what kind of laws or policies we have to facilitate or limit police use of facial recognition, the Clearview AI example is a good example of, right now, we have good data protection laws, but that is subject to change. We've got more legislation going through at the moment that might really restrict the Information Commissioner Office's powers and role so there's no saying that if this situation were to happen again, we would have the same kind of enforcement mechanism and hefty fines imposed on Clearview. But it is also a good example of the patchwork of legislation that we have. And this is the patchwork of legislation that until the Bridges case was what the police, the government, the courts were saying that the police were able, they were saying that was why the police were able to use the technology and that it was adequately regulated by existing statutory provisions and other legislation. So just to give an example of what that legislation looks like and which we argue, and eventually the courts found, was not the case,

they were relying on things such as their police common law powers, the Data Protection Act for the biometrics and personal data aspects. For the equality issues, the Equality Act, the human rights aspect, the Human Rights Act and other legislation to cover things like the covert use of facial recognition, so the regulation of the Investigatory Powers Act and the Protection of Freedoms Act for the CCTV camera use. And so it was our argument, and also the Court of Appeal found in Bridges, to agree, that this existing legal framework was, as they said, "fundamentally deficient". So that's really positive obviously. It means that the combination of these standards was not sufficient governance. But we would obviously also argue there is no governance that would ever be able to mitigate for the rights infringed by facial recognition. And I think that's a really important distinction because the court in Bridges, the Court of Appeal, identified that whilst the existing legal framework wasn't sufficient, what we've seen is that police and the government have started to try and fill those gaps. So, for example, we've seen Surveillance Camera Commissioner guidance, we've seen codes of practice, we've seen the College of Policing has issued more guidance on facial recognition so they're definitely taking note of the judgment and trying to fill in the gaps where the court said it wasn't sufficient. So ultimately, the police are considering not whether we should use facial recognition but how we can use it and trying to bring it into alignment with the law, post Bridges.

[...] the fact that they can use it, however they want, is problematic but Liberty's perspective is that the harms of facial recognition can never actually be mitigated for, and this is especially true in light of what I spoke about earlier with respect to this UK government's creeping authoritarianism. It's not even creeping anymore, it's very blatant [...]

"And I think the lesson here and we will hopefully go into some of the, you know, what can we learn from each other in the fight against this technology. But the lesson here is really the limits of strategic litigation. We were always aware that, you know, we weren't going to be able to win the political argument in a courtroom, and using the law often only helps once the infringement has been made. So I think that's a really important take away that the law has to continue to be the floor and not the ceiling, particularly because facial recognition is already in widespread use.

"So, for us, our primary concern is that not having an explicit legal basis is problematic. We still agree and we're obviously really proud of the win in Bridges because it identified the existing legal framework wasn't

good enough and that's obviously a problem because it means, you know, as we've identified, the police just use it however they want. They use it to, they say, they will allege that they use it to catch particular people, terrorists, etc., which we are also really critical of, because, as we've already spoken about, the concept of crime and the concept of a lot of these things is heavily racialised, is heavily classed, so it's not as black and white as, you know, you can use it to just catch these people. But, obviously, the fact that they can use it, however they want, is problematic but Liberty's perspective is that the harms of facial recognition can never actually be mitigated for, and this is especially true in light of what I spoke about earlier with respect to this UK government's creeping authoritarianism. It's not even creeping anymore, it's very blatant but it's really not difficult to see who the use of this technology will continue to fall upon in various moral panics this government has. So yeah, I think I'll leave it there and over to you."

Gil Gan-Mor: "The reason we knew about the police using facial recognition is that we caught the police using an LPR system, licence plate recognition which records automatically the movements of cars in Israel and we filed a petition to the High Court of Justice in Israel, saying that it's illegal and they do not use such a system of general authority of the police, they need a specific authorisation to use such a mass surveillance system and the court sided with us. So when the police wanted to start using facial recognition and we know that they already have the system because in the last Pride parade in Jerusalem, they officially asked the Attorney General to start using facial recognition during the parade in order to protect the people that were attending the parade and the Attorney General said 'no'. I think it's because of our case against the use of the LPR system.

3 ways to backtrack on FRT

1. Move the discourse from the police to the political system: FRT must be brought to the parliament, there is currently insufficient legal basis and rights protection for it to be implemented.
2. Proportionality: technology adopted to identify criminals in a strict context has no business being used out of this context.
3. Rethink police oversight bodies with tech in mind: a new independent oversight body on police is needed to address the use of data by law enforcement, a body that can monitor and limit what police do with data.

"But I think Ben was talking about: should we try to ban these technologies or what can we do? My basic approach is, if we could convince the government and the police and the other agencies that we should continue without these technologies then that could be the best; if we could ban the technology, that would be the best. But I don't think it's realistic. And I think that we already see a lot of police and law enforcement agencies around the world, and also in the democratic world, are already using facial recognition systems. So what can we do? I think we should follow three principles.

"First, we should try to stop this pattern that we see, and Ben also talked about it before, the pattern, that these technologies are being deployed secretly by these law enforcement agencies without anybody knowing about it, without public discourse, without any transparency. The first thing we need to do is move the discourse from the police to the political system. And we can do it using litigation because we can, for example, say that there is no sufficient legal basis and stuff like that and that usually works to shift the issue to the parliament and then we can have a public debate.

[...] the traditional oversight systems that we had for the police are not good enough for the new technologies.

"And then we can talk about, this is the second principle, about proportionality. I think this is important to try to address the more severe effects of this technology and not just oppose it, as a whole for example. It's different if we use facial recognition to just recognise people on a watchlist that is carefully selected by authorized people with maybe a judicial authorization or something like that. Or if we are using the technology to just identify everybody that is walking in the city square or something like that, or it's different if we're talking about severe crimes or we are talking about, just, regular crimes, that maybe this technology should not be used to solve just regular crimes. And these are the questions that we should try to raise and to limit the fact of the technology.

"And the third principle is oversight. I think that the traditional oversight systems that we had for the police are not good enough for the new technologies. We need something else. We cannot keep on going with the traditional system of police going to a judge, getting the warrant and then that's fine. I mean there's supervision but maybe later they will just give some statistics to somebody who is overseeing the police, it's not enough. I think with these kinds of new technologies that can surveil

so many people, easily, we need to think about independent bodies that can oversee the law enforcement agencies that will have independent status, that will have the power to get all the information they need to see actually what the police are doing with these technologies and I think that may help reduce some of our fears about these technologies."

Brenda McPhail: "The last question for the panel which is: what is your advice for us, here in Canada? We are facing a really important moment in this country from a policy perspective, in that we have our private-sector privacy law being revised right now, currently in second reading before parliament. We're told that another, our public sector, federal public sector law, will soon be revised. And we also have a new Artificial Intelligence and Data Act on the table, before our parliament. So taking into account that we may here have an important window to advocate for change, legislative change, what should we be learning from your experience? What's your advice to us at CCLA, and to the members of the public, who are here today because they're interested in this topic, and maybe interested in seeing what they can do as individuals, through political engagement or other ways, in order to address the risks of this technology. And Ben, I'm gonna start with you please?"

Ben Wizner: "Coming from the United States, I don't advise any country on private-sector privacy laws, because we basically don't have them, except in certain sectors for medical records, for education records, we don't have any baseline consumer privacy law in the US at all. In part, because the sort of dominant data collection companies are very powerful political actors in the US. But also, in part because we have a Supreme Court that has very broadly interpreted the Constitution to make private sector regulation quite difficult. So our focus is on the government and law enforcement side.

[...] what you want to be doing with law and policy is actually creating inefficiency. Creating inefficiency, that when we're talking about the exercise of state power, efficiency is a feature and not a bug. And we need to find ways: if we're going to use these technologies, slow them down dramatically.

"And the principle that we have tried to convey both to the public and the courts, is that we need the law to play a role that we didn't need in the past. In the past, our privacy was protected more by cost than it was by law. There simply wasn't an efficient way for governments to keep track of most of us or even many of us. And if they wanted to know where we

were, they might have to have teams of agents following us around, they certainly didn't have any technologies, like the ones we're talking about right now. And so it was a resource question for them. And that acted as a very powerful limitation. And when we're in a world now, where it's technologically and financially feasible for governments to collect and store records of all of our movements, communications, we need law to do something that we didn't need before.

Now we walk by, in the US, certainly in cities, we walk by surveillance cameras, dozens of times a day. We have learned not to worry about that very much. And there's something rational about not worrying about it, because in almost every instance, no one will ever look at that footage. But that's the way things were, that's not the way things will be. Because pretty soon those cameras are going to be fitted with AI capabilities, with detection mechanisms that are looking for suspicious behavior and that will send an alert to someone.

"We need law to create that friction that used to be created by cost. Usually, that means interposing some kind of warrant requirement, making sure that there is a neutral magistrate in between a decision by an agent to pursue us and the collection of that data. That doesn't always map perfectly onto these technologies. But what you want to be doing with law and policy is actually creating inefficiency. Creating inefficiency, that when we're talking about the exercise of state power, efficiency is a feature and not a bug. And we need to find ways: if we're going to use these technologies, slow them down dramatically. I think with the public, you know, obviously everyone who works on privacy and surveillance has the same complaint: How do you convince people that this is an urgent issue that affects them?

"Now we walk by, in the US, certainly in cities, we walk by surveillance cameras, dozens of times a day. We have learned not to worry about that very much. And there's something rational about not worrying about it, because in almost every instance, no one will ever look at that footage. But that's the way things were, that's not the way things will be. Because pretty soon those cameras are going to be fitted with AI capabilities, with detection mechanisms that are looking for suspicious behavior and that will send an alert to someone. When they also have facial recognition, they'll send not just an alert, but an identity. So that thing that you walk by every day, imagine that being a person looking at you, and it's going to change the way it feels to move around in our society. You can convey

that. Security technologist Bruce Schneier likes to say, 'think about how you feel when you're driving and a police car pulls up right next to you. Think about how you would feel if it were that way, all the time'. And we have to kind of train ourselves to feel that way all the time and if we don't want to feel that way, all the time, then we need to use law and policy to prevent us from having to live under that kind of regime."

Security technologist Bruce Schneier likes to say, 'think about how you feel when you're driving and a police car pulls up right next to you. Think about how you would feel if it were that way, all the time'.

Brenda McPhail: "Manuel, what's your advice for Canada?

Manuel Tufró: "Well, I really don't think we could have advice for you because I think with all the problems that maybe you have here, I'm sure that the oversight structure you have is better than ours. I think that the standard for accessing information is better than ours. But what our experience would say is that implementing chaos and lack of oversight makes good grounds for strategic litigation. But, of course, that's not enough. Because there's another point we all here want to raise regarding technology itself. And so there's the problem, how can we access information to do that? But I think Gil talked about three points that were very interesting. I would like to add a fourth point maybe, or I'm asking myself if we should think of a fourth point. I was listening to what Ben was saying about Clearview AI. And he emphasized a couple of times, that it's a startup company, a new company, that did not recognize some limits that big corporations maybe have. So that means that the very dynamic of the business, the security and the technological business is pushing the limits. And there are serious economic incentives for these enterprises to cross all limits. So I was thinking maybe we should reach out to corporations, too, not only work with the legal and the political system, but find a way to reach out to corporations to talk about this. I don't know. I'm asking myself, after hearing what is being said here today."

Brenda McPhail: "Thank you. Gil, did you have anything to add to your advice, in addition to your three points that we should be thinking about?"

Gil Gan-Mor: "I don't think I can advise Canada. I came here hoping to learn from you, actually! But I think that what we need to think about all the time is that we cannot just talk with the courts or talk with the officials in the government, we also need to talk with the public. And we

also need to try to figure out a way to make the public understand the best of these technologies. And I think all of our organizations are struggling with this because the idea of privacy is always something that is difficult to make people understand until they don't have any more privacy. It's not something that is very clear to people when they don't understand what can happen to them until it happens. And so maybe we should not only talk about privacy, maybe we should talk about civic space. We should talk about how we actually want to be living? What is going to be our lifestyle, in the future when these technologies are in our lives? Will we feel comfortable going to a demonstration, when we know that our name will be on a list somewhere, easily? Will we feel comfortable going to a gay bar, if we know that this can be recorded somewhere? Are we feeling comfortable about a situation where a technological indication can get us arrested? I mean, it's not just about privacy, it's about how we feel in this 1984 kind of world where everything and everyone can be identified, and it can be recorded somewhere, and somebody can use it? And I think when you're talking to the public about these feelings, maybe they might be more receptive to the concerns."

Brenda McPhail: "I feel strongly, we sometimes say, if you wouldn't want someone standing at the corner taking your fingerprint to let you cross the street, or why are you okay with the camera essentially taking the print of your face in that same situation? I think those kinds of examples, that bring it home, are helpful. The police car right beside you is another great one. But taking it beyond privacy, taking it to 'what kind of world do we want to live in' is such an important point to be made. So, thank you. I wanted to give, on this International Women's Day, the last word to our other woman on the panel. But first, I just want to remind our audience that after the end of this response, we will be turning to questions. So if you have questions that you'd like to enter into the Q&A, please feel free to do so. With that, Emmanuelle, what's your advice for us?"

[...] if you wouldn't want someone standing at the corner taking your fingerprint to let you cross the street, or why are you okay with the camera essentially taking the print of your face in that same situation?

Emmanuelle Andrews: "What a lovely way to introduce the end and now I'm under a lot of pressure to do all the women proud! But I did actually want to pick up on something Ben said, which was about 'slowing things down'. There's a reflection from the Bridges case that I think is a really good example of slowing things down. This was the fifth ground

in the court case, which we were successful in. So the police and public bodies in the UK have a positive duty to have due regard to the need to eliminate discrimination. Now that's obviously often used as a tick box exercise. It's just a due regard, they don't need to actually eliminate it. In the instance of Bridges, this became incredibly crucial. So, in the case, what we argued was that the police did not satisfy themselves that they had adhered to this legislation, because, as the Court of Appeal, said, they never sought to satisfy themselves either directly or by way of independent verification, that the software program does not have an unacceptable bias on the grounds of race or sex. So, just to explain what that means, the court agreed that because the police had never actually looked at the technology, and tried to figure out whether it would be racist and sexist, they therefore were not in adherence to their duty to try and have due regard to this fact. So, this is relevant insofar as basically what the court is saying is that when police are deploying facial recognition, they can't simply rely on the manufacturers' kind of statement of 'oh, it's really accurate and oh, don't worry about whether it's racist, or sexist, or whatever', the police have to actually certify that themselves. So, that's a good example of slowing things down because to do that will take a long time, and is costly, and so on.

"And that also leads me on to my second point and it's kind of a nice contrast, because I think slowing down is in a way, like a short-term way of trying to fight against this technology. But I think we also really have to be playing the long game and the long game is the really nuanced conversation that we all need to be having to upskill the public and ourselves about the issue of racial injustice.

"Because, as we've discussed, this technology is being used in particular ways to oppress marginalized communities. And I should say, not just racial injustice, but injustice in all forms, oppressive in the kind of wider sense. And in the case of police it will always be deployed to oppress and harm the most marginalized people. And obviously, that's different to the bias arguments that I referred to in the first example. So I think, for Liberty, not only are we working against facial recognition, but we're also working on a big, longer term campaign, that is really attempting to get to the heart of encouraging the public, encouraging everyone to think more critically about how we conceive of crime, and that we have to deal with the root causes, before we jump to allegedly sophisticated and technological quick fixes. This tech is expensive and we're asking: what would it look like if we invested that money into communities? And that's helpful, because parliamentarians will always say, how can we afford to make our schools better or house homeless people? Well, we can use facial recognition, as the example of 'well, why don't you just

ban facial recognition, let's use that money to actually respond to the social issues that the police are justifying their use of facial recognition to police and control communities in the first place?' So that's obviously a really long-term strategy. But I think we need to have really creative strategies that do work on the kind of short, medium term, so legal cases and strategic litigation, but also really to try and win on those really public, political conversations."

Brenda McPhail: "Large-scale, systemic, societal change seems like a great turning point for us to address some of the questions that are starting to come in from our audience. I think, for reasons of time, and also to get through as many audience questions as possible. I will read the question, and I'll ask the panel to volunteer if they're interested in responding to that question. And we'll perhaps just have one, or at the most two, panelists for each question to make sure that as many audience members as possible, have their questions answered.

"The first question from one of our participants. He or she states, 'Today, it's facial recognition. Tomorrow, it's my voice or gait. Facial recognition is one of several ways that allows companies to commodify our biometric information and use it for their own purposes'. What's the panel's response to that overall concern? Any takers?"

"I know that you've (to Emmanuelle) done some work in terms of other kinds of biometrics, and I think this questioner is asking about, you know, raising the issue, that it's not just about faces, because there are other ways in which our bodies can be used to identify us or work against us in these contexts. Have you got any comments on that?"

Emmanuelle Andrews: "Yeah. I can't wait to hear what the other questions are because that was already such a good question. I know, there's gonna be so many amazing ones. But I think this is a really good example, actually, of an also, just kind of referencing the context in Canada that Brenda mentioned, which is that there's an opportunity to potentially win some things around privacy and so on. I think, yeah, this question is so important, because it identifies that exactly as the question it started with: it's facial recognition today, but what is it tomorrow? And I think one lesson from the challenge of trying to fight facial recognition is that it has happened at such a fast pace and we've all been trying to catch up with it, that I think what we really need to do is is to get in front of the many different types of forms and future kind of technical innovations that are coming down the line. And I think, of course, you know, we can't always presume to know what that technology might look like. It's, as we say, very innovative and things are happening at a very fast

pace. But I think there is a way, certainly, to try and stop it by kind of legislating for really broad bands so saying biometric technology should never be used by the police, for example, would be able to capture not just facial recognition, but also gait recognition. And yeah, other forms of biometric surveillance essentially. So I hope that starts to answer the question. But yeah, it's a great question."

Brenda McPhail: "I've another question from our online audience but I would also like to extend the opportunity to my INCLO colleagues, who are sitting in the room, that if you have questions, put up your hand, and we will have somebody get a microphone to you. So the next question from our online participants: 'What can we, the public, do to protect ourselves from the archiving of our faces by governments or corporations? For example, while going through the airport here at Pearson in Toronto, I was forced to use the automatic customs machine to get back into Canada. The machine then scanned my face. I can only imagine this image is now kept in some archive, along with other past scans of my face. So, what can we do as members of the public to push back against the collection of our faces for state purposes?"

[...] one of the things that we should try to do is to expand the knowledge of people about the risk of giving voluntarily their biometric data to corporations.

Gil Gan-Mor: "You can donate money to the Canadian Civil Liberties Union. That's, I think that's a very good idea! But I think one of the things that we should try to do is to expand the knowledge of people about the risk of giving voluntarily their biometric data to corporations. We saw that in Israel during the COVID pandemic where facial recognition high-tech companies were viewing the situation as a very nice opportunity to advance their product. One example was that they started to sell it to football stadiums and theaters, or large-crowds facilities, saying, 'OK, if you want people to come to your venue quickly, without having to spend a lot of time checking if they have their green passport to show they were vaccinated - during the time of those Covid restrictions - then we can give you a biometric system. People will identify themselves when they arrive at the stadium, they will stand in front of our camera and the camera will say, "this person is free to go in, you don't need to check him again, he's already uploaded his green passport or certificate to our website".

"And a lot of people said, 'oh good, I can skip the line. I don't need to wait in lines'. They don't understand that what they are doing is giving their biometric data to some company that nobody knows what they are

going to do with this photo bank, recognised photo bank, in the future. Nobody reads the restrictions in their privacy policy, which usually say that they will not use it, but in the future they may use it some way. Or nobody is thinking about a lot of cases that we saw recently of these photo banks being stolen from this company, or there was some failure in protecting them.

"If you lose your credit card or somebody steals your credit card, you can change your credit card. But if your biometric data is in the hands of some corporation, you can't change your biometric data, this is something that is unchangeable. So people should be really aware of the risk and we should try to explain to people that even though it's legal to give it voluntarily, just don't do that or be aware of the risk of giving away your biometric data."

Brenda McPhail: "I don't see how many hands in the room. The offer is still out there. Next question from an online participant: 'Of course, facial recognition technology should bother us from a privacy and civil liberties viewpoint. But is there anything good about it? Can we think of any way facial recognition could be used to protect or reinforce our freedoms?' Ben's got his hand out?"

If you lose your credit card or somebody steals your credit card, you can change your credit card. But if your biometric data is in the hands of some corporation, you can't change your biometric data, this is something that is unchangeable.

Ben Wizner: "Well sure, I mean most technologies have beneficial uses, I don't want to see a surveillance drone flying over my neighborhood. But I might want to see it flying over a warzone and recording human rights violations, I might want to see a news organization fly one over a violent encounter between the police and protesters and to record that. Similarly, with facial recognition, it could be used to identify a war criminal, it could be used to identify a child victim of a grotesque crime. We shouldn't pretend that these technologies don't have use cases that we wouldn't applaud. Of course, that's really true of government power, and a lot of other iterations. A lot more crimes would be stopped if we allowed, as the city of Baltimore and the United States tried, to fly a spy plane over the city all day, and really record everything in granular detail and record that for months so that it could be rewound by the police to solve crimes that happened.

"But do you want to live under a spy plane? Where every time you walk down the street holding hands with somebody that is going to be in a surveillance time machine that can be rewound later on? Yes, more crimes are going to be solved, but it's going to change what it feels like to live in our societies. And that's what makes these arguments so difficult and it's why putting constraints on facial recognition is going to be so difficult because I think, candidly here, the government's got caught a little bit flat-footed, like they expected people to be enthusiastic about their use. And I think they're going to organize more and they're going to try to identify more and more cases where it was used. And you saw Clearview AI very ghoulishly stepped into the Russia/Ukraine war and said, 'Well, we'll identify the corpses of Russian soldiers so their mothers won't have to be in doubt'. Right. So, they're just trying to find ways where we'll think, 'Oh, these people are on our side'. But again, it doesn't help us to ignore that there are uses of these technologies that can be helpful and beneficial."

Brenda McPhail: "Which is why it's so important, as you said earlier, to think about if these technologies should be used and if, then when and how? But that 'if' question needs to be at the forefront. I think we have time for one last question: 'Would it be fair to say that as such programs' effectiveness or usefulness evolves, democracy itself, as we define it, is directly and peripherally undermined, regardless of a nation's governance status?' That's an awesome question. Anybody want to take a stab? You're nodding, Manuel."

Manuel Tufró: "I would just say that yes, it's fair to say that. I think Gil made a very clear point about that, when he argued that it's not like only a privacy issue, it's a broader issue and we have to address it in all its complexity. I think it feeds into other problems, which affect democracy, too. So I think, definitely, yes, we could say and we should say that it's a threat to democracy."

Brenda McPhail: "I apologize to all those questioners whose questions we can't get to, but we are running very close to the end of time for this panel. And we do appreciate that an hour and a half on a Zoom call is probably more than long enough for many of you who are likely ready to log off and go for dinner. So, I just want to conclude by thanking our panelists. Thank you, Manuel, and Ben, and Gil and Emmanuelle, for sharing your insights and your experience and your advice and your stories with us because one way that we come together to fight incursions into rights, is by sharing stories that help us understand what's at stake. So we're so grateful that you were willing to share your stories with us today. I'd like to thank, on behalf of CCLA, the International Network

of Civil Liberties Organizations for supporting this panel, for bringing everyone together, and allowing us to have these conversations with special thanks to those individuals and you know who you are, who did all of the behind-the-scenes work to make this happen? I think that all of us here at the table, many others at INCLO, are committed to carrying forward work to stand up for rights and freedoms and civil liberties, and to serve as some of the identifiable faces of resistance to the potential for mass surveillance, to serve as experts in policy circles and settings, to advocate against invasive uses of FRT here in Canada, to have nuanced conversations around those 'if' and 'when' questions.

"And we invite those of you in the audience today to share that work with us. Whether it's through political engagement, whether it's through individual action, whether it's just through as as Gil so articulately explained, simply continuing to learn more about this and other risky technologies, and make choices, make conscious decisions about whether or not you are or not willing to participate in those systems, particularly those that are risky, that impact our privacy rights and all of the other suite of rights that privacy enables. With that, we'll bring this to a close. Thank you very much, everybody."

[...] make choices, make conscious decisions about whether or not you are or not willing to participate in those systems, particularly those that are risky, that impact our privacy rights and all of the other suite of rights that privacy enables.