HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

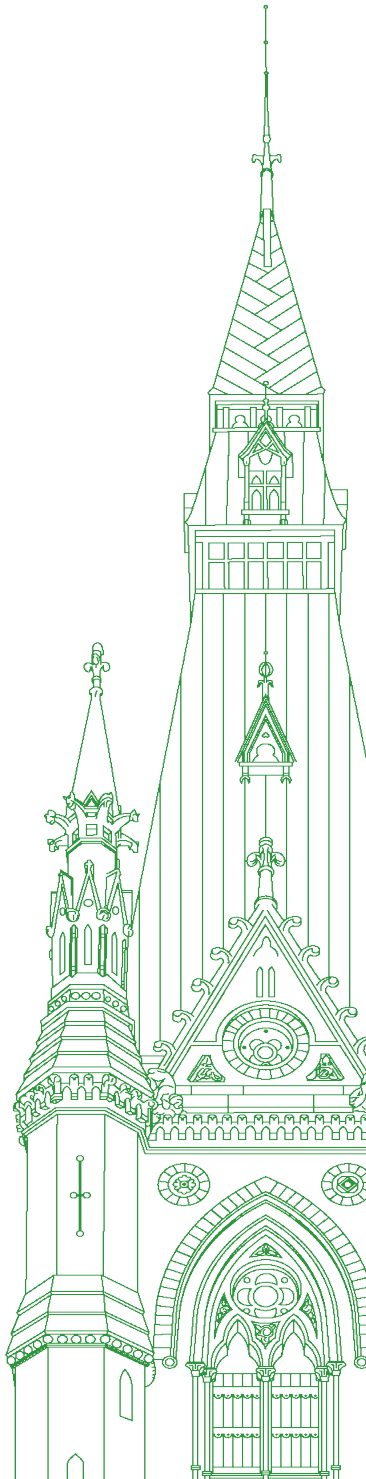
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 008

Thursday, February 17, 2022



Chair: Mr. Pat Kelly

Standing Committee on Access to Information, Privacy and Ethics

Thursday, February 17, 2022

● (1535)

[*English*]

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

Welcome to meeting number eight 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 Thursday, January 13, 2022, the committee has commenced its study on the collection and use of mobility data by the Government of Canada.

Today's meeting is taking place in a hybrid format, pursuant to the House order of November 25, 2021. Members are attending in person in the room and remotely by using the Zoom application. The proceedings will be made available via the House of Commons website. The webcast will always show the person speaking rather than the entirety of the committee.

Before we go to witnesses, a study budget was distributed to all of you. Are there any objections or questions?

I see none. Shall the budget be adopted?

(Motion agreed to [*See Minutes of Proceedings*]

The Chair: Now we can proceed directly to hearing from our witnesses.

In the first panel, from BlueDot, we have Dr. Kamran Khan, chief executive officer and founder, and Mr. Alex Demarsh, director of data science.

You have five minutes for your opening statement. Please go ahead.

Dr. Kamran Khan (Chief Executive Officer and Founder, Professor of Medicine and Public Health, University of Toronto, BlueDot): Thank you, Mr. Chair.

Good afternoon, everyone. Thank you for the invitation to participate in today's session.

As you just heard, my name is Dr. Kamran Khan. I am BlueDot's founder and CEO. I'm joined by my colleague Alex Demarsh, who is BlueDot's director of data science.

I'd like to begin my opening remarks with some background information to help provide some important context for today's conversation.

First, I'm an infectious disease physician and have been in clinical practice for the past 20 years. You may recall that 20 years ago a novel coronavirus that the world had never seen or heard of before emerged in Guangdong province in China and rapidly spread to more than two dozen countries around the world, including Canada. That virus was SARS-CoV. I started my career in the midst of that outbreak, and it is an experience I have never forgotten.

It has been the inspiration for everything I have done in the past 20 years of my career as a practising physician, including the past two years of this pandemic when I have been managing hospitalized and critically ill patients with COVID-19; as an epidemiologist and a professor studying outbreaks of emerging diseases and how they spread in our increasingly interconnected world; and as an entrepreneur who founded BlueDot eight years ago to harness the power of global data and modern digital technologies to strengthen our ability to respond to rapidly evolving outbreaks.

I'd like to be clear that BlueDot is an organization that produces infectious disease insights, not one that collects location data from mobile devices. Our sole purpose and reason for existence is to protect lives and livelihoods from the growing global threat posed by emerging infectious diseases.

To fulfill our mission, we procure and analyze diverse worldwide data from publicly and commercially available sources to better detect signals of outbreaks around the world at their earliest stages, to forecast their patterns of spread to cities around the world and to empower local responses that mitigate their health, economic and social consequences.

With COVID-19, we did just that. Our technology used publicly available data to detect a worrisome outbreak emerging in Wuhan back in late December 2019. We then accurately forecasted the global pathways of that outbreak through the worldwide network of flights, publishing our findings online in the world's first peer-reviewed scientific study on COVID-19.

When COVID-19 began to spread here in our own country, we analyzed de-identified GPS location data that we procured from third party providers that we selected because they adhered to Canadian and other internationally stringent privacy laws and regulations and had strong data privacy practices in place.

These third party providers collect GPS data from mobile apps that have a logical need for location. The apps require express consent to use location data and provide users with the opportunity to withdraw such consent at any time. Note that any location data we receive from these third parties has been de-identified before it ever reaches our organization.

Some of these de-identified location data are also pre-aggregated before we receive them, while some data are delivered at the device level. We have never attempted to connect device-level data to an individual. We have no purpose for doing so and we are contractually prohibited from making any attempts to do so.

Working with the Public Health Agency during this pandemic, we have analyzed and transformed de-identified GPS location data into actionable public health insights to help anticipate epidemic surges, to inform where and when the utilization of finite resources will have the greatest impact on saving lives, and to understand the effectiveness of social distancing interventions, all under rapidly evolving emergency conditions.

Throughout our engagement, we have taken careful steps to ensure that any data or insights we have delivered to the Public Health Agency could not conceivably be associated with any individual.

I founded BlueDot because 20 years ago, as a frontline health care worker, I watched a virus cripple an entire city for four months. I understood then that more disruptive outbreaks would follow, and they have, with greater frequency, scale and impact.

Two years into this pandemic, I am certain that data, analytics and technology can help us stay ahead of outbreaks that we will inevitably face again and protect lives and our way of life. I am equally certain that we can continue to realize the value of such public health insights in a manner that fully respects and protects data privacy.

Thank you again for the invitation to be here today.

The Chair: Thank you for your impeccable timing on your five-minute statement.

We'll begin our rounds of questions with Mr. Kurek.

Mr. Damien Kurek (Battle River—Crowfoot, CPC): Thank you very much, Doctor. I appreciate your testimony today.

To start off, I was interested when in your opening statement you talked about data that was procured from apps that required express consent to be given for location tracking. In regard to the data that was sent to the Public Health Agency of Canada, do you know how many mobile devices and/or individuals had data collected that was then sent to PHAC?

● (1540)

Dr. Kamran Khan: Through you, Mr. Chair, to the honourable member, on the data we collected in the context of the Canadian response to the COVID-19 pandemic, it was approximately five million devices in total.

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

This committee was provided with a slide deck that appeared to be a presentation that would have been given to the Public Health Agency of Canada. Along with that slide deck was a letter from the Parliamentary Secretary to the Minister of Health. In that slide deck, the maps and whatnot had very, very interesting information that I'm sure was helpful in developing policy, but the explanatory slides at the end of that document state, and I quote, "Weekly values of active device users at the province and health region level can be downloaded directly from the BlueDot mobility dashboard."

Can you tell the committee what this data looks like before it's uploaded to the dashboard, and what information is accessible to the dashboard? First, though, did the Public Health Agency of Canada have access or subscribe to access to that dashboard?

Dr. Kamran Khan: Alex, do you want to take that question?

Mr. Alex Demarsh (Director, Data Science, BlueDot): Sure.

Through the chair to the honourable member, on the first question, we provide analytic reports of population-level mobility metrics via reports like the one you reviewed. We additionally make the same kind of metrics available through a dashboard that the agency can use to view the same kind of analysis directly themselves.

In no case is there individual device-level data shared with the Public Health Agency of Canada. It's additional summary metrics of the type that are outlined in that report. It's supporting data, but in a format that they can use to answer more dynamic questions rather than questions we've predetermined and included in our reports.

Mr. Damien Kurek: Thank you, Mr. Demarsh. Just to be clear, the Public Health Agency of Canada did subscribe, or had access, to this dashboard that's referred to.

Mr. Alex Demarsh: That's correct.

The dashboard, to be clear, includes only our summary metrics, not the original data, but yes, they do have access to that data via the dashboard.

Mr. Damien Kurek: Certainly it's interesting. Part of the concern that's been highlighted by privacy experts is the ability to reidentify and to gain access, and the privacy concerns related to this information.

Is there any possibility that we can see that data?

Mr. Alex Demarsh: Just to clarify, do you mean the contents of the dashboard we shared with the agency?

Mr. Damien Kurek: Yes. Would the data available on that dashboard be available for this committee to see?

Mr. Alex Demarsh: Certainly. Yes. We can follow up in writing with a sample that would inform you of the contents of the dashboard.

Mr. Damien Kurek: Thank you very much. That's much appreciated.

With regard to the check-ins, the slide deck specifies "anonymized device movement in half-hour windows, at the bottom of the half hour". As well, a device can have up to 48 check-ins per day, and devices with fewer than eight check-ins per day are removed from the sample.

Can you explain the context? That's a tremendous amount of information. Can you provide detail as to how BlueDot ensures that there is no way for that data to be reidentified?

Mr. Alex Demarsh: Dr. Khan, unless you'd like to jump in, I'd be happy to take this one.

Dr. Kamran Khan: Sure. Why don't you go ahead?

Mr. Alex Demarsh: To start, every question we're seeking to answer is about populations. These data are only useful in so far as they inform us indirectly about average contact rates in populations. We have no interest in individual devices. The information's only useful in aggregate.

The data are de-identified, so in most cases they're pre-aggregated metrics and summary statistics about those populations. When we do receive individual device level data, there's no identifying information received. The contents of it are simply an approximate location and a time-stamp.

The description of half-hour reporting only pertains to that data we hold in extremely secure internal secure data processing platforms, with only a limited number of internal users having access. We have a number of reasons for using industry best practices for data security.

Beyond that, to your larger point about potential reidentification—

● (1545)

The Chair: Thank you, Mr. Marsh. We are out of time for Mr. Kurek's round.

Just before we go to Ms. Hepfner, I would ask you, Dr. Khan, when speaking, to perhaps hold your microphone a little bit closer to your mouth. It doesn't appear that you have a boom. We'll see if we can get better audio for the interpreters.

With that, please go ahead, Ms. Hepfner, for six minutes.

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

I also want to thank the witnesses for being here today and helping us refocus on the question that we're addressing in this motion, which is specifically about the data that public health received, in part through BlueDot.

I'd like to just keep you talking, if you don't mind, Alex, about this.

What specific data did public health get? You said, approximate locations and time-stamps, so it's all general information. Is there no way that public health could look at this data, in any way reidentify it and know that Lisa Hepfner was shopping at Lime Ridge mall on the weekend?

Mr. Alex Demarsh: Absolutely not. To clarify even more, even approximate locations and time-stamps are not a level of data we share with the agency. It's further aggregated, either by the geographic range and larger populations where the device was found, or over time periods of a minimum of 24 hours. It's still more generic and unidentifiable than you've described.

Ms. Lisa Hepfner: Dr. Khan, maybe you could comment a little bit, from your expertise, on how valuable this data has been in helping the government fight the pandemic, and maybe what it would have looked like if we hadn't had this data.

Dr. Kamran Khan: To the honourable member, thank you for that question. It's a really important one.

With traditional public health data, we count things like cases, hospitalizations and deaths, but when we're dealing with a rapidly evolving outbreak, by the time we see a case, we're already too late. There are a whole bunch of things that have already transpired. There has been, at some point earlier, a contact, an exposure. The person exposed might develop symptoms and get tested. By the time they get their test results back, we're already very far behind.

The entire use for these types of data—again I want to highlight de-identified, anonymized data—is ultimately to estimate contact rates in the population. That's what this is all about. It's just estimating how much contact is occurring in the population, because contacts are a leading indicator of what is coming next. Cases tell you that something has already happened in the past. It's a shift from being reactive to being proactive and anticipatory.

What we don't want is to be behind an outbreak. We want to try to get in front of it. We want to try to change the course and trajectory. Pretty much everything we're talking about here really comes down to one thing: trying to inform public health about contact rates in the population and where they're increasing in a way that is a precursor to exposures, cases, hospitalizations and deaths, so that an intervention can happen.

I've been working in the field of emerging outbreaks for my entire career. We know that outbreaks spread quickly. It means that we have to be able to react, understand and move even more intelligently and in a better coordinated manner.

My sense is that, as a physician, I can take care of one patient at a time. These types of analytics can support the public health response that could be impacting not only lives but all of the economic and societal implications we've had to endure for two years.

● (1550)

Ms. Lisa Hepfner: Is there any other way to get this data?

Dr. Kamran Khan: I don't believe so.

There have been discussions about things like the use of synthetic mobility data. I do want to highlight that much of those types of approaches are actually using empirical location data as a training dataset. Secondarily, in a very stable environment, that might make sense, but keep in mind the last two years have been anything but stable—constantly changing conditions, new variants and new public health interventions and policies. This has been a very erratic two years, and empirical data are going to give us the best foresight into what is coming next so that we can make intelligent decisions about how to mitigate the health, economic and social consequences.

The last thing I would say is that BlueDot—and my work as a physician for the last 20 years—is about protecting lives but also protecting data privacy. This is something that we take very seriously and is really at the core of what we do as an organization and, candidly, why I founded BlueDot in the first place.

Ms. Lisa Hepfner: I would ask our witnesses to go into a little more detail about the extent that they go to to protect the privacy and security of this data.

Dr. Kamran Khan: I know time is limited.

Number one, any data we receive is de-identified before we receive it. Internally, we have a whole bunch of procedures, both administrative and security procedures, to manage and keep the data in a secure environment. Any outputs that we then actually analyze, produce and deliver to the Public Health Agency are aggregated in a very thoughtful way so there's no conceivable way we can envision that any of this data could be reassociated with any individual. From the very beginning of how we receive the data, how we store it, how we process it, how we aggregate it and how we deliver it, we're doing that in a very thoughtful manner in the entire process.

The Chair: Thank you.

Ms. Lisa Hepfner: Very good.

The Chair: With that, it's now time for Monsieur Villemure for six minutes.

[*Translation*]

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

Dr. Khan, Mr. Demarsh, thank you for joining us today.

I am sure of the benefits you are talking about for public health. I also understand that you are not compromising people's privacy. You are applying best practices with the data you receive.

My concern is about the consent of the user, who probably clicked on “I accept” somewhere, usually without having read the conditions or having failed to understand them.

Do you think users understand that their data is used by a third party?

[*English*]

Dr. Kamran Khan: Mr. Chair, perhaps I can take that question.

The Chair: If either of you want to answer, go ahead.

Dr. Kamran Khan: Thank you for the really important question.

Here's what I can say. I can't speculate as to what is in each person's mind when they are providing express consent to enable location data. What I can say is that they do have the opportunity to withdraw that express consent at any point in time. I think it is an important question around the consent process. In our work with third parties, we have ensured that the organizations we're working with are adhering to all of the Canadian and other internationally stringent privacy laws and regulations, and that they have strong data privacy practices in place. They have assured us in writing around some of their practices. We've done our due diligence as well in making sure we're working with partners that are respecting privacy.

With respect to the consent process, it's an important question and conversation about whether the consent is sufficiently informed. I'm not an expert in that domain, but I am sure this committee will, through all of the experts who have presented, be able to arrive at a better assessment of that.

[*Translation*]

Mr. René Villemure: Thank you very much for your answer.

I know that this is not your area of expertise, but my concern is about the distinction between people who may know that their data is being used and those who understand this. There is a distinction between knowing this and understanding it.

Do you think the members of our committee have reason to worry about the entire process?

● (1555)

[*English*]

Dr. Kamran Khan: To the honourable member, my response would be that this process is one that requires some careful thought. Within the diligence that is happening through this committee, it is certainly appropriate to be asking the question as to whether we are striking an appropriate balance.

I think we've all heard that these types of data can be protecting lives, can be protecting a lot of lives and protecting society, not just from COVID-19 but, as I mentioned in my opening remarks, we know there are more of these that are coming. I think the diligence that is happening here with this committee is appropriate, looking at and just asking whether the processes can be better.

If there's anything we can do in response to a pandemic, or anything else, it's really just to learn from our experiences and look at ways that we can do things more optimally.

That's my input as a physician.

[*Translation*]

Mr. René Villemure: I have no doubt that you are saving lives.

Did you choose Telus as a supplier or was that the Public Health Agency of Canada's decision?

[*English*]

Mr. Alex Demarsh: Mr. Chair, I can respond. To clarify, Telus is not a data supplier for us. We have no relationship with Telus.

[*Translation*]

Mr. René Villemure: Where does the data you use come from?

[*English*]

Dr. Kamran Khan: We have two data suppliers that provide us with data. In our agreements with those suppliers, we have contractual obligations that, if we do make any public statements, we would just need to seek their permission first before making any announcement.

If there was a request for us to do so, we'd be happy to approach our suppliers to seek that permission.

[*Translation*]

Mr. René Villemure: I completely understand the context.

I would like you to send to the committee the names of your suppliers, using the appropriate precautions, of course.

So there is no direct contractual relationship with Telus. Can you tell us what kind of businesses provide you with data, without naming them?

[*English*]

Dr. Kamran Khan: First of all, we are not working with Telus. That is not the source of the data.

The data we've been working with comes from providers that use GPS location data from mobile apps. Again, through that process I described of consenting to use location or being able to withdraw consent—and again, these are providers who are following all of the data privacy laws and regulations in Canada and in other international jurisdictions—largely these are providers that are actually interfacing with mobile apps.

[*Translation*]

Mr. René Villemure: Thank you very much.

[*English*]

The Chair: Mr. Green, go ahead for six minutes.

Mr. Matthew Green (Hamilton Centre, NDP): Mr. Chair, in preparation for this committee study and anticipation of the witnesses, we spent some time looking up the bios and we came across Mr. Demarsh and noticed that he had been employed by PHAC until March 2021.

Can Mr. Demarsh share a little about his role with PHAC and elaborate on how this informs his work now with BlueDot?

Mr. Alex Demarsh: Certainly.

I was an epidemiologist, data scientist and manager of data engineering teams at the agency for years. In the context of the pandemic, I worked in the emergency operations centre, building and refining data systems used for more traditional public health data. I was aware of BlueDot and had worked with BlueDot's software in a previous role, but at that time had no interaction or involvement with BlueDot's work. I was working in a completely different part of the agency.

I will say, if the question is why I joined BlueDot, I was persuaded by the mission and excited about the technology and the possibility of really making a difference in public health. That informs my work and our interaction with the Public Health Agency of Canada, but I had no direct involvement in contracting or the agency's decision to work with BlueDot.

● (1600)

Mr. Matthew Green: In the final points I think he raises an important question, which is why I wanted to put it on the table, given the committee that we're in.

Just to assure the committee, at any point when you were working with PHAC, would your information or contribution as an employee of the federal government have contributed to the procurement process of this contract?

Mr. Alex Demarsh: No. It would not, in any way whatsoever.

Mr. Matthew Green: Okay. Thank you for that.

In his introductory remarks, Dr. Khan listed “entrepreneur” on top of his medical expertise. Does the doctor have any comment on the commodification of personal data as it relates to BlueDot's business model?

Dr. Kamran Khan: Thank you for the question.

BlueDot's business model is about using and driving innovation to protect lives. I want to highlight that BlueDot's entire reason for existence is around developing innovation to prepare for and respond to not only the threat that we've been enduring for the past two years, but also the many before and the more that will come.

As a physician with 20 years in practice, as I highlighted in my opening statement, I've had experience on the front lines of crises, which has really informed how I see where the world is headed. As an academic and as a scientist, I've been studying outbreaks my whole professional life.

Creating BlueDot was less about creating a business and more about creating a vehicle—

Mr. Matthew Green: Could we get clear about exactly what the business model is?

How is it that you have been able to take the subject matter expertise as a frontline physician and recognizing, hopefully, the support and the need for the privacy of health information, even in the instances of pandemics...? In which way did you find this an opportunity where there could be commodification in a profit model or motive for this particular point in time?

Dr. Kamran Khan: To respond to that, BlueDot has a for-profit business model. We use any revenues that we are generating for the purpose of reinvesting back in job creation, in innovating and in developing better solutions and technologies, as I mentioned, for detecting, assessing and responding to outbreaks.

I also want to highlight that BlueDot is a certified B corporation, a type of social benefit corporation that is oriented around social good. I've chosen that business model because it is an opportunity to scale the impact that we could have—

Mr. Matthew Green: Thank you.

I have two questions that are a bit more specific.

We've heard the conversation about there being the approximate location and a time-stamp. How approximate is the location of the data?

Mr. Alex Demarsh: GPS data is not located at a precise point in space. It's—

Mr. Matthew Green: In the weekly reports on mobility trends that have been prepared by and received from BlueDot, among other things, the percentages are shown of increases and decreases in time spent in a home and in outdoor gatherings, the number of movements and other measurements.

How would you arrive at these percentages if it's just an approximation of where they are? You would have to have residential-level analyses.

Mr. Alex Demarsh: It's an excellent question. That's a good example.

The specific analysis of “home” is not a reference to a home in the sense of a person's home. It's the primary location of the device, defined as a zone of about 600 square metres. The purpose of that analysis is to distinguish devices that are staying close to their primary location, versus those that are moving about, as a proxy for contact rates in the population.

Mr. Matthew Green: It's pretty safe to say that people bring their cellular devices with them wherever they go, so 600 metres seems to be, although approximate, a fairly small circumference.

I know that I'm out of time, but I look to revisit this line of questioning in my next round.

Thank you.

The Chair: Thank you, Mr. Green. You'll have the opportunity to do that, but first we will go back to Mr. Kurek, who is possibly sharing his time, I understand.

Go ahead, Mr. Kurek, for five minutes.

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

One of the concerns I have.... I represent a rural constituency, where population density is significantly less than in major urban centres. Are there specific protocols in place to ensure that those who may live in rural Canada have their privacy protected?

● (1605)

Dr. Kamran Khan: Do you want to take that one?

Mr. Alex Demarsh: Yes. I'm happy to speak to that one.

Our general practice is to aggregate either by time or by a geographic boundary defined by population for all analyses we supply to the agency.

In the case of a rural setting, the smallest geographic boundary would be defined by the underlying population as calculated by Statistics Canada. That would be a relatively large spatial area. However, we would still, in that situation, only report statistical summaries, numbers of devices, proportions and percentages. There would be nothing conceivably identifiable or associated with an individual device, or anything like that.

I would reassure a rural constituent that there's no prospect of identification, even in that setting.

Mr. Damien Kurek: Thank you.

I appreciate the information and look forward to receiving the more detailed information that's available on the dashboard.

Specifically in terms of your relationship with PHAC, we learned quite recently from the Privacy Commissioner that they were not consulted in regard to the acquisition of mobility data.

Did that come up in the conversations that took place over the course of BlueDot's relationship with the government?

Dr. Kamran Khan: Thank you for the question.

Over the course of the relationship with the Public Health Agency, the issue of privacy did come up on many occasions. We had that conversation directly with the Public Health Agency about procedures and how we were working with the data and so forth. Certainly, I wouldn't have full knowledge of how the Public Health Agency may have spoken to the Privacy Commissioner. I can't speak to that specific piece, but between BlueDot and the Public Health Agency, this was a topic of discussion over the course of the relationship.

Mr. Damien Kurek: Thank you.

In terms of the siloing of data, certainly it's logical that the Public Health Agency of Canada would need data to develop policies related to pandemic response. Was the data that BlueDot provided subject to a siloing where you were assured that the data would only be used within the Public Health Agency of Canada or is it available for the Public Health Agency of Canada to possibly share with other departments?

Dr. Kamran Khan: I'd have to go back to our specific agreements and contracts. Our work with the Public Health Agency of Canada was largely for the agency to be able to support local, national and provincial...and these types of decisions across the country.

To my knowledge, I'm not entirely aware of what the agency may have done and how they may have shared this with other jurisdictions across the country. We provided data to the Public Health Agency for the purposes of better coordination across the country in terms of the response to the pandemic.

Mr. Damien Kurek: Thank you for that.

I'm curious if you have a relationship with other levels of government, whether municipal or provincial, in your work here in Canada.

Dr. Kamran Khan: Yes, we do. Any of the work we have done with regard to COVID-19 response in Canada, and in particular around these types of data, have only been with public health institutions in Canada at the provincial and municipal levels.

Mr. Damien Kurek: I have one quick final question.

There was a RFP for continued collection and use of mobility data that spoke to postpandemic uses. The government delayed that RFP to increase competition. I'm curious as to why BlueDot didn't submit a proposal with that RFP that's now been delayed by the government.

● (1610)

The Chair: I'm terribly sorry, but I'm going to have to ask the witness to deliver a five-second response or else return to it in a future round.

Please go ahead.

Dr. Kamran Khan: We are not a mobile device location data business. We are simply an infectious disease insights business. I believe that RFP was more oriented towards cell tower based data.

Mr. Alex Demarsh: To be clear, that RFP was exclusively about cell tower data, which we don't possess, so we're not eligible for that RFP.

The Chair: Thank you.

Mr. Bains will be next for five minutes.

Go ahead.

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

Thank you to our guests, Dr. Khan and Mr. Demarsh, for joining us today. My questions are coming to you from Richmond, British Columbia.

I wanted to talk a little bit about the opt-in clause. The more comprehensive the data is, the more useful it is. What effect does the opt-in clause have on the usefulness of a dataset? Either witness can respond.

Mr. Alex Demarsh: I'm happy to speak to this.

In this context, because the data are only de-identified location information, there's no degree of consent for additional information. We never receive anything beyond the de-identified location or aggregated summary metrics related to movement. For this purpose, there's no notion of degree of consent or additional information that we could obtain per device or in aggregate.

Mr. Parm Bains: I asked a previous witness a similar question: If they had indicated that it would have been better to have an opt-in versus the opt-out, I'm just wondering if it would be useful. The data does not appear to be useful if we do have the opt-in.

Mr. Alex Demarsh: I

Mr. Parm Bains: It's the usefulness of the data. Would that make the data not so accurate in terms of the kind of data we're collecting if it were an opt-in? Maybe people just wouldn't be doing it.

Mr. Alex Demarsh: I see.

Mr. Chair, I do think that it's probably true in the general sense that opt-in policies usually result in fewer people opting in than opt-out policies do. I think that is true as a general statement.

Mr. Parm Bains: Okay.

Your website states that BlueDot was one of the first organizations in the world to detect the risk of COVID-19 and alert its clients. How did BlueDot identify the emerging risk of COVID-19 before anyone else did?

Dr. Kamran Khan: Mr. Chair, I'm happy to take that question.

This, I think, comes back to the fact that BlueDot is an infectious disease insights organization. The work we're doing with mobile data is just one small piece in what we do.

What we have developed is a platform that is monitoring online publicly available sources, currently in 65 different languages, using things like machine learning to help pick up early signals or clues that there may be an outbreak occurring in a particular area of the world maybe before it's actually officially reported. That is something we have developed over years, because ultimately we know that time is everything when you're trying to respond to an outbreak.

Our platform detected it back in late December of 2019, and, as I mentioned in my opening remarks, knowing that there's an outbreak is one thing, but actually understanding its potential for global spread is another. That's something that we also do, using the data on the worldwide movements of flights through the global airline transportation network that we all live in. We in fact published the world's first peer-reviewed study accurately predicting where COVID-19 would start to spread. That was back in early January of 2020.

I think this gives you a sense, hopefully, that as an organization we are looking at this problem holistically, from early detection to assessment and to emergency response.

● (1615)

Mr. Parm Bains: Thank you for that.

Further to that, what efforts did you make to comply with Canada's privacy legislation?

Dr. Kamran Khan: Mr. Chair, I think I'll try to take that.

Certainly, any of the data we are working with is de-identified. It is not associated with any information about names, addresses, occupations, nationality or any data of that sort.

In relation to the work we have done with population mobility data, we have ensured that we're working with providers that are following Canadian and other international privacy laws and regulations and have had a chance to get assurances and do our own diligence on the data privacy practices they had in place.

Mr. Parm Bains: Thank you, Dr. Khan. That's all I have.

The Chair: Yes, you're out of time, Mr. Bains.

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

[*Translation*]

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

Before I begin, I would like to let the witnesses know that they must have the equipment provided by the House, as the interpreters are struggling to hear what is being said. I hope this won't count against my time.

Dr. Khan, your testimony was fascinating. I would like to draw on your 20 years of experience and have a broader discussion. What do you think about the exploitation of data in general, which, through a surveillance capitalism of sorts, can influence and change a population's behaviour?

Do you see surveillance capitalism as dangerous?

I understand that what you are doing is very good, but I am calling on your overall experience.

[*English*]

Dr. Kamran Khan: Thank you for the question, and apologies for my perhaps suboptimal mike. I hope you can all hear me okay.

This is certainly a broader question and an important question. I will say that we really believe that our purpose—this is what I can speak to—is a noble purpose. We are using business as a vehicle for social good and social impact. It is—

[*Translation*]

Mr. René Villemure: I will interrupt you, Mr. Khan, as I am convinced.

Based on your experience and your knowledge, do you think data exploitation can constitute surveillance capitalism that influences and changes a population's behaviour?

[*English*]

Dr. Kamran Khan: I do think there are concerning uses of data in some forms that can influence behaviour and certainly can have negative social impacts. I would agree with that statement.

As to my personal feeling, I don't believe that the work we're doing falls into that particular domain. However, I would agree broadly, as a general statement, that the statement you made is fair.

[*Translation*]

Mr. René Villemure: Thank you very much, Dr. Khan.

I have no further questions.

[*English*]

The Chair: Thank you.

We will go to Mr. Green.

Mr. Matthew Green: I'd like to take a moment to pick up where my colleague from the Bloc left off to get a better understanding of this from both Dr. Khan and Mr. Demarsh based on their respective experiences.

We're going into this new frontier of digital epidemiology or surveillance to hopefully help change habits in a way that is beneficial to the public. I'm wondering, from your experiences, what is too far. What are the boundaries that, ethically, we should not breach and that would respect the privacy of people's health and well-being versus the balance of societal good?

Dr. Kamran Khan: Mr. Chair, perhaps I'll try to take that question. It's a big one. It's an important question.

The identification of individuals and personal information obviously requires a different level of consent. Drawing from my own experience with informed consent, when I'm talking to a patient about having a surgical intervention or something, I have to make sure I'm explaining all of the risks and benefits. As it relates to personal information, an additional level of rigour is certainly required.

I want to highlight some of the earlier comments. Our goal is not to.... We are not directly looking to change individual behaviours. We are generating public health insights to inform and empower the public health community to make—

● (1620)

Mr. Matthew Green: I'll just interject. If I could, I'd like Mr. Demarsh to add, given his experience at PHAC.

Mr. Alex Demarsh: I would agree with the general statement. There are widely accepted additional requirements when data could be associated with an individual in any conceivable way, and certainly in medicine and epidemiology, when private health information is included, there are additional levels of scrutiny and security.

I'll just clarify that BlueDot does not hold any personal information across any of our holdings, in mobility data or beyond. We don't have any private health information in our system in any sense. That would require substantially more investment in privacy and security, and different trade-offs between goods such as public security in the context of a pandemic and other valid goods, like personal privacy.

The Chair: We will go now to the final two questioners, MP Patzer and MP Khalid, for five minutes each.

Go ahead, Mr. Patzer.

Mr. Jeremy Patzer (Cypress Hills—Grasslands, CPC): Thank you very much, Mr. Chair.

I'm going to start by asking you how many countries you are collecting data from.

Dr. Kamran Khan: The question is about data. Do you mean data in general or...?

Mr. Jeremy Patzer: Yes, I guess just generally speaking, because as you talked about, it's not just a Canada-based package. You're getting datasets from across the world. How many countries is it, approximately?

Dr. Kamran Khan: I would say that for mobility data—and I'd have to look up that number—it's probably most of the world in some form. Obviously there are certain areas where there may be more devices and more data. We are looking at global airline and transportation data across the entire planet, as we are trying to detect early signals of outbreaks. We are doing this in multiple languages across the world. This is really a global problem and requires a global view of this kind of risk.

Mr. Jeremy Patzer: Okay. That's obviously an enormous amount of data that requires a lot of server capacity.

Where are all the servers that host all that data? Are they all here in Canada, or where are those servers located?

Dr. Kamran Khan: Alex, did you want to take this one?

Mr. Chair, neither of us is the technical leader. We have our head of technology. Everything that we have is managed in highly secure cloud environments. We have full levels of encryption. We work with independent third parties to enhance our data security practices. We have administrative and operational procedures with how all our data are managed.

Alex, I don't know if there's anything else you wanted to add.

Mr. Alex Demarsh: We would have to check the geographic locations of the physical servers that our cloud providers use in our case.

It would be Canada or the U.S., and we'd confer with our head of technology to be sure. I'd be happy to report back with a definitive answer.

Mr. Jeremy Patzer: The reason I'm wondering is that the context of this study is de-identified data. We've seen other reports that between 90% and 95% of individuals who had their data de-identified can be re-identified.

The reason I'm asking is that quite often data is only as secure as the person who's trying to find it. When there are multiple avenues, that's what I'm trying to get at here.

I guess this would be a broad, industry-based question, and we see breaches of security within the government from time to time. We see it in the private sector from time to time, and quite often, actually. Industry-wide, what risks are there to this data being taken by a nefarious character?

Mr. Alex Demarsh: Mr. Chair, we've spoken to our general cybersecurity and data security practices. As the honourable member will be aware, innovative Canadian start-ups need to be quite conscious of data privacy, as our innovations are globally sought after for a number of reasons. It's top of mind. We use industry best practices, select secure cloud environments, internal auditing, access control processes and multifactor authentication. These are the normal suite of cybersecurity practices required by our type of business.

● (1625)

Mr. Jeremy Patzer: I've one more question here for you guys.

The federal response plan in April 2021, under the heading of surveillance, states that:

> COVID-19 surveillance is a pan-Canadian initiative...numerous data [systems] including existing surveillance systems with novel, non-traditional data sources.

It sounds like a lot of things going on. It's a very vague, very broad definition for surveillance.

Is there any issue that a definition like that might be too all-encompassing, too broad, and not narrowly focused enough for the framework of what you guys are doing, which is providing specifically for infectious disease?

Mr. Alex Demarsh: If it's helpful to clarify, in public health, surveillance is used as a catch-all term for infectious disease case data or other disease case data.

I'm not certain which document he's referring to, but that is a general term well understood within public health collection of data about individual cases in the context of an issue of public health importance.

The Chair: I'm afraid that's time.

For the final round, we have Ms. Khalid for five minutes.

Ms. Iqra Khalid (Mississauga—Erin Mills, Lib.): Thank you very much, Mr. Chair, and thank you to the witnesses.

Perhaps I'll start with Dr. Khan.

Dr. Khan, how helpful do you think this collection of mobility data was in shaping a good response to the pandemic in Canada?

Dr. Kamran Khan: I think it was actually quite helpful. As I was describing earlier, the counterfactual, or how this would have played out in the absence of these types of data, would have been trying to catch up after we saw that cases were surging in a particular area. This is a leading indicator by being a proxy of contacts that are forthcoming.

I will say that in our anecdotal assessments of the past two years, we've seen many instances of the analytics that we have generated and provided to the Public Health Agency being precursors of subsequent surges or providing really important actionable insights.

What I think, and I say this as a scientist, is that to answer that question appropriately and fully would require a full retrospective after the pandemic is over to understand what worked and what didn't. Just as in any other instance, there's an opportunity to learn from this.

The simple answer is that I think a lot of lives were positively impacted and benefited from this type of work. This is notwithstanding the importance of privacy, which we're discussing here today, but I do firmly believe it had a very strong impact on protecting lives and livelihoods across the country.

Ms. Iqra Khalid: Thank you.

Dr. Khan, what would be the impact if PHAC stopped using this type of de-aggregated, anonymized data to inform health policy in Canada?

Dr. Kamran Khan: I will start. Alex, feel free if you would like to add your thoughts.

The metaphor I might use is that it provides some timely insights in a rapidly evolving outbreak. The metaphor of not having that information in those types of insights is a bit like fighting an outbreak but with a bit of a blindfold on. For example, if there's a public health intervention on social distancing, you may not even know if it's working, and if it is, whether it's having the intended effect and where, when and how to adapt.

I think in many ways, if I'm just looking at it purely from a public health perspective, lack of these insights could really compromise the public health community's ability to respond to this type of threat.

Alex, is there anything you would like to add?

Mr. Alex Demarsh: No, I think that's right. It would be removing a tool that's useful in the context of us, as a public health community, not having many tools. Beyond that, I'm not sure. I think Dr. Khan gave a comprehensive answer.

Ms. Iqra Khalid: Thanks very much for that.

Are you satisfied with your company's policies and protocols around the protection of privacy? Are you satisfied with the government's protocols, including in the RFP in the contract and the role and importance that privacy played within that?

● (1630)

Dr. Kamran Khan: Let me start out with our own privacy practices. We are always interested in striving to continuously improve and enhance in areas where we can.

I will say I am quite comfortable and proud of all of the work we have done to ensure privacy at BlueDot, starting with only working with data that has entirely been de-identified from providers that are following the privacy laws and regulations. We're being very thoughtful on how we generate it out to share with the Public Health Agency.

I do want to note that we had been preparing for this years before the pandemic emerged. That gave us the opportunity not only to develop the technical capability but also to have rigorous discussions and develop policies and standard operating procedures on how we would work with these types of data in a crisis. I think we have been very thoughtful throughout the entire process.

I'm probably not well suited to speak on behalf of the Public Health Agency and the RFP.

The Chair: With that, I'm going to bring this panel to a close. We're just a minute over time right now, but I do want to thank our witnesses.

I will suspend, and we will, hopefully, turn this around as quickly as we can for panel two.

● (1630)

(Pause)

● (1634)

The Chair: I call the meeting back to order.

I would now like to welcome everybody to the second panel.

Welcome to our witness. I understand we have one witness from Telus. From Telus Communications, we have Pamela Snively, vice-president, chief data and trust officer.

You have five minutes for your opening statement. Go ahead, please.

● (1635)

Mrs. Pamela Snively (Vice-President, Chief Data and Trust Officer, Telus Communications Inc.): Thank you for the opportunity to provide this committee and Canadians with the facts about our Data for Good program.

Telus launched Data for Good in April 2020 because we believed, as we still do, that our company's responsible use of data can play an impactful role in making more evidence-based and informed decisions. We created Data for Good to provide de-identified—that is, essentially anonymous—data to assist governments and health authorities in their efforts to stem the spread of COVID-19 and better understand the impact of interventions like restrictions and stay-at-home orders.

Data for Good was a natural extension of Telus's broader commitment to using our technology to enable social good in support of Canadians and the communities in which we live and work.

As you heard from Dr. Tam, the Data for Good program provided critical insights that supported more informed policies. In short, it worked.

I want to make one thing perfectly clear, Telus did not share any personal information with government—not one iota. Telus always puts its customers and their privacy first. At no time have we ever relaxed any of our rigorous policies about our treatment of personal information, including when we launched Data for Good during the pandemic.

The Data for Good program operates on a data analytics platform called Telus Insights, which is the only privacy-by-design certified platform of its kind in Canada. This platform uses de-identified datasets to reveal movement trends and patterns while protecting individual privacy. Under the Data for Good program, we allow data scientists from our partners, including the government, to have supervised and guided access to our secure Insights platform, which contains only de-identified datasets from our mobility network. Those datasets never left our systems. The data of our customers, even de-identified data, was not sent to the government.

I want to pause on privacy by design. That Telus Insights is privacy-by-design certified is important. Privacy by design is the international gold standard for privacy protection. It was developed here in Canada by Dr. Ann Cavoukian. Privacy by design goes beyond the requirements of the law to entrench privacy protections into the design and operation of the IT systems, networks and business practices of an organization.

With this certification, our Data for Good program is independently validated as being rigorous in its privacy protections. You also heard Dr. Cavoukian's endorsement of our approach last week.

We have taken a leading role nationally on the development and promotion of de-identification as a critical process to enhance privacy protections. Telus is a founding member of CANON, the Canadian Anonymization Network, whose mission is to promote effective de-identification practices and includes the leading Canadian de-identification experts.

Our commitment to de-identification is at the core of Telus Insights. Thanks to our privacy-first approach, Telus was able to leverage our Insights platform to provide pandemic assistance through Data for Good while fully protecting the privacy of customers. While some may compromise on privacy during a public health emergency, we did not. We are very proud of Data for Good and we were intentional and explicit in our public communication about the program.

We developed and published on our website five core data use commitments on how we would share de-identified data and protect privacy. These accompanied a full description of our program along with an FAQ. We had a banner on the main Telus website that linked to this information. Before and after launching the program, we did op-eds and interviews with The Globe and Mail and other Canadian media outlets and published news releases announcing new collaborations. We later publicized that Data for Good was awarded the International Association of Privacy Professionals Privacy Innovation Award in November 2020.

Apart from our public-facing communications about Data for Good and Insights, we consulted with the Office of the Privacy Commissioner of Canada on our transparency plan. We provided that office with an overview of our program, including the five core commitments. The OPC provided valuable feedback, which we gratefully incorporated.

The final point I'd like to make is that as part of our effort to go beyond simple compliance with the law, we offer our customers the ability to opt out of our data analytics program. We see this as a reflection of our customer-first commitment.

In closing, I want to reiterate that Telus provided access to this de-identified data for the public good. The data contained no personal information, so the privacy of our customers was respected, and we made great efforts to be transparent about the program. All of this is consistent with Telus's long-standing track record of protecting our customers' privacy.

Thank you again for the opportunity to speak with you today. I'd be pleased to answer your questions.

The Chair: Right, and with that we'll begin with Mr. Kurek for six minutes.

● (1640)

Mr. Damien Kurek: Thank you very much to our witness for joining us here today.

I found it very interesting and I'm hoping you can unpack a little about what you meant when you said that data was never sent to government.

I'll give you context for the type of response I'm hoping to get. This committee was provided with a letter from the Parliamentary Secretary to the Minister of Health with a slide deck from BlueDot as an example of some of the information that had been provided to PHAC from that organization. We have not been provided with a similar dataset or information as to what the data looked like that Telus had provided to the government.

I wonder if you can elaborate on what it means when you say that it was never sent to government.

Mrs. Pamela Snively: Absolutely. Thank you for the question.

What I meant by that is that we don't actually send data to the government. The way our program works is that we allow data scientists from our partners to come onto our platform, our de-identified data platform, for supervised and guided access. There, they are able to do the queries that are consistent with the use and purpose that we've discussed with them and that needs to fit with our program, and then they're able to create derived data, or what we call “insights”.

When I talk about an insight, the best thing to do would be to picture a heat map or a graph, a bar chart or line graph that would show movement patterns or trends. After they've done that and pulled out these insights, they would be able to download them. Before they could take them, we would review them to make sure they were consistent, that they met all our reidentification risk metrics and that they were consistent with the purpose for the contract, and then the government would be able to take that derived data or insights with them.

Mr. Damien Kurek: In terms of officials from the Public Health Agency of Canada who went to Telus Data for Good, was it a specific location or virtual location? I'm curious as to exactly what that means.

Mrs. Pamela Snively: It is a virtual location, so they're not physically on the premises. It was data scientists coming onto our platform. We provide guided, supervised access to our platform, but it is virtual.

Mr. Damien Kurek: I'm sure all of us around this table have mobile devices, and there is a tremendous amount of information that is available and exists within the cellular providers that operate within our country, and there has to be a high level of trust there.

I'm curious as to whether you would be willing to share some of what that data looked like when it was sent to the Public Health Agency of Canada.

Mrs. Pamela Snively: Yes, I can certainly take that away and we can share sample reports of what the data would look like.

Mr. Damien Kurek: In terms of those who were able to access the platform, we've heard from some experts that de-identifying and the ability for data to be reidentified is very much on a scale. Anonymized and de-identified data can be names and cell numbers taken out of a dataset, or it can be synthesized in a way that would make it virtually impossible for that to be reidentified.

Can you highlight exactly what the officials from the Public Health Agency of Canada, data scientists or whatever the case was, were able to see when accessing your platform—not just the reports, but what were they able to see?

Mrs. Pamela Snively: It might be more relevant for me to say, actually, what they weren't able to see. That would be any information about any identifiable individual. The way the platform works is more query-based. It's not as though they go on and see a bunch of data. What they're able to do is develop queries and get back information and insights drawn from that de-identified data. That might be a clearer way of describing what they would see when they would come onto the platform.

● (1645)

Mr. Damien Kurek: Hypothetically, the government could then ask.... Let's say there was a sporting event, or they could look at grocery stores or movement during a certain time of the day. Those are three hypotheticals, but those are the sorts of queries that the government would be able to make of the system and the data set.

Mrs. Pamela Snively: Perhaps you could clarify your question. If you're looking for movement during a particular sporting event, yes, but not in real time. One of the controls that we have on the platform is not to provide any real-time data, because that increases the risk of reidentifiability to something. It would no longer be considered de-identified.

Mr. Damien Kurek: I'm out of time, so maybe I'll follow up again later, but thank you for answering the question.

The Chair: Thank you. Now we have Ms. Saks for six minutes.

Ms. Ya'ara Saks (York Centre, Lib.): Thank you, Mr. Chair, and thank you to our witness today. I look forward to hearing your answers to some of my questions.

I listened to your opening statement, and I've also heard from Dr. Ann Cavoukian, who was recently here. She raved about how well-developed the Telus Insights offering is, and being built by privacy by design at the forefront of this platform, your work sounds critical in offering insights that go beyond in protecting any identifying data.

From what I understand, PHAC never had access to any personal information. How did you make sure they did not have access to this personal information? This is my first question. Then I'd like to ask how privacy by design protects privacy, and since you do have the certification, how rigorous was that process?

Mrs. Pamela Snively: Thank you very much for those questions.

To ensure that PHAC or others on the platform do not have access to personal information, we went through a very rigorous process. It actually took years to build the Insights platform to be what we wanted it to be. We realized years ago that there could be tremendous value in this de-identified network mobility data. We're talking about the pings that devices make off of the cell towers as they move about the network. If we could de-identify those pings and just look at the movement patterns, there were a number of "social good" uses that we could immediately see, with tremendous value, and we've seen that borne out during this pandemic.

We consulted with leading de-identification experts and spent a tremendous amount of time building the technical platform and the technical rules to de-identify the data and strip the identifiers, but we went far beyond that to rules around the way the queries are made and controls on the frequency with which queries are made, as well as considerations of geography and aggregation. There were a number of different technical and statistical controls, and then on top of that we put in administrative controls.

I talked earlier about the guided and supervised access. That's another administrative control that we have in place whereby we're actually supervising what is happening on the platform and reviewing what is taken from the platform, as well as strict contractual controls prohibiting reidentification. Those are some of the ways we control and make sure that we have reduced the reidentification risk to a very small risk.

In terms of the privacy by design certification, I'm glad you asked about that. We're really proud of that certification. It is a very rigorous process. Our most recent privacy by design certification for the platform was just before COVID, so it was excellent timing for the launch of Data for Good. It took over four months to conduct. It's conducted by a fully independent external audit group.

There are seven privacy by design principles. Those turn into 30 privacy and security criteria, and then into 94 different controls that are illustrative of our meeting those criteria and principles. It took, as I say, about four months. They complete that report, and then they have to take it to an independent accreditation board to have it independently reviewed before we can be certified.

● (1650)

Ms. Ya'ara Saks: In other words, it was an extremely rigorous process and a priority before PHAC could even access any of the data on the platform in a supervised fashion.

Mrs. Pamela Snively: That's correct.

Ms. Ya'ara Saks: Mr. Chair, how much time do I have?

The Chair: You have almost two minutes.

Ms. Ya'ara Saks: The intent of Telus' Data for Good and the program was to help PHAC understand and fight this pandemic. From where I'm sitting, it sounds to me that tremendous care has been taken by Telus's Data for Good to make sure the data is de-identified, which certainly is reassuring to me and is reassuring to Canadians now that you've just described the very rigorous process for certification.

From what I understand, the data that was collected from Telus's Data for Good was supervised and reviewed before it was released. It was then posted each week on PHAC's website, so there was a level of transparency with Canadians of this data, which I think also seems very beneficial as we communicate with the public why this information is so important in managing the pandemic and using data as a tool.

Can you speak to how the Data for Good program supported the COVID 19 response from your perspective of being engaged in this search process with PHAC?

Mrs. Pamela Snively: I'm not privy to all of the uses to which the data was put. We have a record of them, but I don't know them all personally.

We heard Dr. Tam speak earlier about how valuable it had been to have mobility data and be able to layer that in with epidemiological data, similar to what Dr. Khan was speaking about earlier as well, and to be able to map what had gone on with the contagion and to make predictions about where it might go and be proactive, Dr. Khan said, as well as reactive.

It was also possible to look at the impact of different restrictions and policies to see how effective they were. As we all know, at the outset of the pandemic, a number of different restrictions were placed on us that we hadn't experienced before. We were able to see, by looking at these large-scale movements and trends in patterns, whether or not they were effective in curbing movement.

Ms. Ya'ara Saks: May I ask a yes-or-no question?

The Chair: No, we're way over time.

[*Translation*]

We now give the floor to Mr. Villemure for six minutes.

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

Good afternoon, Ms. Snively.

I have two questions for you. We will try to get them answered in six minutes.

How did you get users' consent to collect their data?

[*English*]

Mrs. Pamela Snively: The data that this is based off of at the point of collection is collected in the course of providing mobility services, so that consent is applied to its use for mobility services and to provide mobility services; however, when we de-identified the data, it was no longer personal information about our customers.

Rather than relying on consent there, what we relied upon was ensuring that we had de-identified it. Our focus was to ensure that we had protected our customers' privacy and that we were transparent and clear about our use of that data.

[*Translation*]

Mr. René Villemure: So you did not get users' consent.

[*English*]

Mrs. Pamela Snively: We did not obtain user consent for this specific purpose. This was not personal information; this was de-identified information, so the information was de-identified and then shared for these purposes.

[*Translation*]

Mr. René Villemure: Before being de–identified, that data was personal information.

[*English*]

Mrs. Pamela Snively: Yes, it was. Before it goes through the transformation, it's personal information.

[*Translation*]

Mr. René Villemure: Okay.

I assume it is normal for a Telus user to expect the company to use their information to improve its service. I understand that. However, I am not sure they expect this information to be used for other purposes.

What are your thoughts on that?

[*English*]

Mrs. Pamela Snively: I think it's challenging to know what anyone expects.

I want to be clear that there's a very critical distinction between personal information and de-identified information. For personal information, we're very focused on consent and the privacy implications, but when it comes to de-identification, the de-identification process itself is what protects privacy. That's our focus there, and that's how we protect our customers' privacy on that front.

When it remains in personal format, our focus might be more on consent. That's generally the primary driver in our current legislation.

[*Translation*]

Mr. René Villemure: Do users consent to having their information de–identified?

● (1655)

[*English*]

Mrs. Pamela Snively: We have a lot of information in our privacy policy and on our website about de-identification. In terms of all of the various uses and the concept of implied consent under our legislation, although under our legislation it's not generally considered that consent is required. We're very transparent about that. We have, I would say, more information than most organizations might have. We have a lot of information about how de-identification works, why we use it, how it protects privacy, and then more information about how we use data that has been de-identified for analytics purposes.

[*Translation*]

Mr. René Villemure: Your website is indeed full of information, but users have to know they need to visit the website to find this out.

[*English*]

Mrs. Pamela Snively: That's correct. As I said earlier, though, we did a lot of op-eds. We did media releases. We were very publicly transparent.

I recognize that some individuals want to know everything that's going on with their data, while some don't want to know anything and some want to know just in time, when they are thinking about it. That is why we take it very seriously to put all of this information on our website. For those to whom it matters and who want to know everything, it's there. For those who might just think about it from to time, it's there when they are ready to take a look at it.

[*Translation*]

Mr. René Villemure: Okay, thank you.

I will use a broad image to ask my next question, which will concern data exploitation in general.

The translation of human experience into behavioural data is what is called surveillance capitalism, which aims to influence and change behaviours. Of course, the source of surveillance capitalism is all the data, yours as well as other data.

What you think about data exploitation for those purposes?

[*English*]

Mrs. Pamela Snively: I'm not positive.

Through you, Mr. Chair, I'm not sure I understand the question.

What do I think about using data for surveillance capitalists? Is that the question?

Mr. René Villemure: Yes.

Mrs. Pamela Snively: I'm aware that data can be used for good and I'm aware that it can be used in ways that are not good as well. It's absolutely, critically important that we're paying attention to how data is used, that we make inquiries, and that we are responsible in our use of data and are transparent about it. That is exactly the model we have followed at Telus.

[*Translation*]

Mr. René Villemure: Okay. I have no further questions.

[*English*]

The Chair: With that, we move one minute ahead of schedule.

I will move now to Mr. Green.

Mr. Matthew Green: Thank you very much.

I'm going to put to our witness that I'm going to ask questions in what might feel like a rapid-fire way. I'm going to ask you to be as concise as you can with your answers so that for the good and welfare of this study, I can move on to the next question. If I happen to interrupt, please don't take it as being abrupt; I have a limited amount of time.

I will begin, through you, Mr. Chair, with asking the witness if the sale of the collected data is a core part of Telus's business model.

Mrs. Pamela Snively: What we're talking about here today is the Data for Good program, which is—

Mr. Matthew Green: If I could, Mr. Chair, I'm going to direct the question. I'm going to ask very specific questions and I'm going to require very specific answers.

Is the sale of collected data a core part of Telus's business model?

Mrs. Pamela Snively: I think I need to be clear about what the exact question is. If we're talking about the Data for Good program, there is no sale involved at all. It's almost exclusively done for free, or at most on a cost recovery basis.

If you're talking about other types of data, just broadly, and whether they are a core part of our business model, I would have to say no.

Mr. Matthew Green: If no, should not a separate form of consent then be required? That is, if a consumer signs up with Telus under the understanding that the core part of the business model is not collecting data and its distribution, should that collection not, under an ethical framework, require a separate form of consent?

Mrs. Pamela Snively: If we were selling customers' personal information, it would require a separate and very expressed consent. We are not selling customers' personal information. We're not sharing customers' personal information. We're sharing insights drawn from de-identified data points drawn off of our cellular network, the number of pings, so that we can map population movements on a large scale to help with the pandemic. This isn't the sale of customers' personal information.

Mr. Matthew Green: Mr. Chair, respectfully, when it's qualified as customers' personal information and the idea of what's disaggregated and not disaggregated.... Again, with the constant emphasis of what consent looks like under current legislation, I would put to this committee that the legislation is currently the problem.

My next question would be whether Telus is only collecting the mobility data of its clients, or does it collect information of other telecom clients who end up pinging its infrastructure?

● (1700)

Mrs. Pamela Snively: For our Data for Good program and Insights model, we are only using the data of our customers.

Mr. Matthew Green: What about for other programs within Telus?

Mrs. Pamela Snively: I'm not aware of another program that is using data in this way.

Mr. Matthew Green: Okay.

It is my understanding that when Telus purchased Babylon Health in the U.K., Babylon operated under an opt-in consent premise, but after the purchase of the app, it was moved to an opt-out consent process. In fact, the Alberta privacy commissioner found that Babylon had not met the requirements of section 7 of the personal information and privacy act with respect to obtaining consent for collection, use and disclosure of personal information unless otherwise authorized.

Why does Telus default to opt-out option for data collection?

Mrs. Pamela Snively: I'm not sure where that information has come from, but Telus has not moved in the.... When we acquired Babylon in January of 2021, we made changes that brought the program under our privacy program, but we did not move anything from opt-in to opt-out. That was not a change that Telus made.

Mr. Matthew Green: Should there be a different standard of consent, for meaningful consent, when it comes to data collection that you share with governments or sell to third parties?

Mrs. Pamela Snively: If we're talking about personal information, absolutely. If we're talking about de-identified information, there's still knowledge and transparency to encourage customer trust and to earn it, but there's no requirement for consent. In fact, it's probably a little bit unrealistic in most of these contexts. What we heard from Dr. Teresa Scassa and what we heard from the Privacy Commissioner was that in the context of de-identified data, consent is really not realistic and it's not terribly helpful.

Mr. Matthew Green: Through you, Mr. Chair, can the witness here today representing Telus state whether or not they're currently collecting mobility data from Koodo and Public Mobile subscribers for the Data for Good program as well?

Mrs. Pamela Snively: Yes, we are.

Mr. Matthew Green: How aware are the clients of these other brands that their data is being collected as well and used in this way?

Mrs. Pamela Snively: The privacy programs merge, so all of the communications have been similar.

Mr. Matthew Green: The Privacy Commissioner stated that the consent cannot be meaningfully obtained from information buried in privacy policies or terms of use. In the witness's opinion, how clear is it for the average person to find an opt-out for data collection?

Mrs. Pamela Snively: Again, it's hard for me to know what is in anyone's mind. When we are talking about an opt-out, and particularly when we're talking about de-identified information, our primary goal is to protect our customers' privacy, regardless of what selection or option they have chosen. That's why we have focused on strong de-identification for our platform and all of the controls we have in place to ensure that privacy is protected.

All of these consent questions relate to customer privacy, and where we've protected privacy in a different way, that's what we've done. We've looked for other alternatives to protect privacy.

Mr. Matthew Green: Thank you.

The Chair: That concludes Mr. Green's round.

Mr. Patzer, you have five minutes.

Mr. Jeremy Patzer: Thank you very much.

You made an interesting comment in regard to the fact that consent is.... I'm trying to remember the exact words you used. It was that in regard to getting de-identified data, consent was either not required or was kind of an inconvenience, more or less, to getting that data.

Could you comment a little more on that? Why is getting consent such a problem when using de-identified data?

Mrs. Pamela Snively: I didn't say it was an inconvenience, but it may not be helpful, if we're talking about.... The concept of de-identification is to remove the ability to trace it back to an individual so that it's no longer personal information. When we are talking about personal information, consent is very relevant. We need consent for the purposes for which we are going to use it. Once we've turned it into de-identified information, part of the process of de-identification is to protect that privacy, so we don't need to go back and get consent.

We did hear from Dr. Khaled El Emam about alternatives for regulating de-identified information, which can be very interesting. In the absence of that regulation, Telus has acquired privacy by design certification to give that assurance to our customers. We do have use-case reviews. We look at the datasets. We've built in a tremendous number of controls to ensure that our customers are comfortable with what we are doing.

● (1705)

Mr. Jeremy Patzer: I get hung up on the fact, though, that the data was personal to start with. You said over and over again that it's okay because you de-identify it and consent doesn't matter at that point, but you still had to get that personal data in the first place.

We've heard about the social good of programs like this, but what about the ethical good of society and of your subscribers, when you're clearly taking personal data without clear consent, even though it's being de-identified?

You said yourself that you need consent for personal data, but you didn't pursue it. Why?

Mrs. Pamela Snively: I want to be perfectly clear: We got consent to collect the personal information to provide our network mobility services. There is no personal information that we have done anything with, without our customers' consent. All of what we have done has been in compliance with the law.

It's once we de-identify the information, so there are no longer privacy impacts on our customer and we've protected their privacy by de-identifying the information, that allows us to be able to use it for these socially beneficial purposes without impacting the privacy of our customers. Absolutely, we put the privacy of our customers first. We would not be doing this if it were actually impacting our customers' privacy.

Mr. Jeremy Patzer: Did you guys ever consider sending a text message to all your subscribers, informing them of the program and what its intended purpose was?

I know you've alluded to posting on your website, or different things like that, where the average person isn't going to go looking for it. Did you guys ever consider using a text message to inform everybody that their data could potentially be used by the government to inform policy decisions that would directly impact them?

Mrs. Pamela Snively: I'm not sure if we turned our minds to that particular solution. We took steps that we thought were appropriate. We were pretty loud about it with media releases in the context of the pandemic and we put a lot on our website.

As I indicated earlier, we had taken all of our five core data commitments to the Privacy Commissioner to ensure that we were properly being transparent about what the program is and giving the right assurances to our customers.

Mr. Jeremy Patzer: As a clarifying statement here, or maybe a reassuring statement here on behalf of Canadians, from the company side, under this program, at what point will the data that the federal government is using be returned to you, or is there an assurance from the government that it will be destroyed and not held longer than is necessary?

Mrs. Pamela Snively: I just want to go back to what it is that the government has. We're talking about heat maps and charts, insights drawn from the data. This is not our customers' identifiable data. Normally if we're sharing actual data, there would be that type of requirement to destroy the data, but that requirement doesn't necessarily have the same import here. Nevertheless, we do have restrictions on the retention of the data.

Mr. Jeremy Patzer: Will you guys be destroying the data, then, that you have collected, or do you guys have a mechanism for your subscribers to reach out to you asking for the deletion or the release of that data that has been collected to the individual directly?

The Chair: You're out of time. I will allow the witness to give maybe a one- or two-word answer, if possible, and then we'll go to Mr. Fergus.

Mrs. Pamela Snively: The de-identified data on our websites could never be provided back to an individual, because it is not identifiable data. We have the identifiable data that we collect originally.

The Chair: Thank you.

We'll go now to Mr. Fergus for five minutes.

[*Translation*]

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

I would like to thank the witness for her presentation.

I have a number of questions for you. I don't want to be impolite, but I know that, owing to interpretation, it will take some time for you to answer my questions.

In your presentation, you said that the information was de-identified. Do you think that your program called data for good is in line with the most stringent criteria of the data de-identification process, according to industry and a number of academics?

● (1710)

[*English*]

Mrs. Pamela Snively: I absolutely think it meets a very high standard. I don't know if the standard is shifting all the time. There are new technologies that are being developed all the time, so this is something that we are constantly reassessing. If there is more that could be done to further minimize the re-identification risk, that's a process that we are always looking at in terms of further controls we could layer in.

However, we would absolutely not have achieved the privacy by design certification if we were not right up there with the highest standards. We also received an international award for privacy innovation at the end of 2020.

[*Translation*]

Hon. Greg Fergus: Yes, you mentioned that.

When Ann Cavoukian appeared before the committee, on the one hand, she lauded your data for good program. However, on the other hand, she was very critical in saying that the government should have ensured that the Privacy Commissioner examined the data you provided to the government.

Are you aware of the standards set by the Privacy Commissioner?

[*English*]

Mrs. Pamela Snively: I'd like to clarify the question. Do you mean the standards used by the Privacy Commissioner to assess de-identification methodologies?

[*Translation*]

Hon. Greg Fergus: Yes, exactly.

[*English*]

Mrs. Pamela Snively: No, I'm not. Those have not been published.

[*Translation*]

Hon. Greg Fergus: So you, as someone who works in this industry and is responsible for this data, are not aware of the standards set by the Privacy Commissioner.

[*English*]

Mrs. Pamela Snively: It's not that I'm not aware of standards that were established; there haven't been published standards about how to de-identify. The data must be de-identified to the point where it's not reasonably likely to be identified back to an individual in order for it to fall outside of the privacy legislation, and on that the commissioner is very clear, but in terms of exactly what his office would be looking for if they were to assess our de-identification methodology, there's nothing published on that.

[*Translation*]

Hon. Greg Fergus: On what criteria are you basing your statement that your system is pretty seamless and that you can be reasonably certain that the data you share is de-identified?

[*English*]

Mrs. Pamela Snively: As I mentioned earlier, we worked very closely with leading de-identification experts, and we have continued our work—because we saw this as so important—to try to develop standards in this space. We work with leading de-identification experts on CANON, the Canadian Anonymization Network, which we co-founded, to continue to push forward the technology around de-identification and arrive at standards. As you heard from Dr. Khaled El Emam, there are standardized industry techniques. There are certain approaches that experts will take, and one of the ways we can test those is to subject the datasets to re-identification attacks and consider the types of re-identification attacks that could be executed.

[*Translation*]

Hon. Greg Fergus: Do you conduct those tests regularly?

[*English*]

Mrs. Pamela Snively: I'm not sure what “very often” would be, but we have definitely done rigorous re-identification tests and attacks, and we've commissioned them. Part of our work with experts was to do that very thing to make sure it was bulletproof.

[*Translation*]

Hon. Greg Fergus: Do you do that once a year?

[*English*]

The Chair: That's all the time we have, Mr. Fergus.

[*Translation*]

Mr. Villemure, you have two and a half minutes.

● (1715)

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

Ms. Snively, I understand that consent is not always obtained at the source itself, and this idea made the Privacy Commissioner rather uneasy.

What do you think must be done in the future to improve that situation?

[*English*]

Mrs. Pamela Snively: In the context of de-identified information, the focus should be on the actual core privacy protections. I think Bill C-11 started down this path that we can do more things with de-identified data, and perhaps the space it had for codes of practice would be a great place to put some of the standards we were just talking about. How can we get comfortable that we're all talking about the same thing around de-identification and raise that standard?

I think the most important thing, as I said earlier, is not to rely on consent, because we're talking about de-identified information, but to rely on absolutely substantial privacy controls that are in place regardless of the choices or selections. We know that choices and selections are challenging, so let's just get it right.

[*Translation*]

Mr. René Villemure: Okay. Thank you.

Were you inspired by the new European regulation, the General Data Protection Regulation, or GDPR?

[*English*]

Mrs. Pamela Snively: There are some great aspects to the GDPR, and certainly we see in it that they have embraced privacy by design, and that's part of what we believe in as well. We've been embracing the privacy by design concept for a long time at Telus.

I think there are some terrific aspects of the GDPR. I also think there are some terrific aspects to our existing legislation. It's been very principle-based. Although old, it has served us quite well, because it is principle-based. It has not been technology-specific and has allowed us to be nimble and agile in the way we've assessed privacy.

[*Translation*]

Mr. René Villemure: Okay.

[*English*]

Mrs. Pamela Snively: Do I think there could be tweaks? Yes.

[*Translation*]

Mr. René Villemure: In the spirit of my colleague's comment, do you think Telus could have adopted a more proactive approach, for example by sending a text message, instead of a passive approach, which consisted in telling users to visit a website?

[*English*]

Mrs. Pamela Snively: Before we start looking at something like a text message, I think there are a lot of considerations that would go into that type of thing. What we tell our customers all the time is to please not respond to a text message from us that you are not expecting, because it could very well be phishing. There are a lot of different considerations that go into texting customers. A lot of customers do not want to be texted, so it's not a simple decision to simply actively reach out to customers. If we were to do that, I'm not sure how it would play out. Our focus is on protecting their privacy.

The Chair: I'm going to have to stop you. I'm sorry.

[*Translation*]

Mr. René Villemure: Thank you.

[*English*]

The Chair: I did actually allow a fair bit of extra time there in recognition of Monsieur Villemure's earlier round, but we really must go now to Mr. Green.

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

Mr. Matthew Green: Thank you.

There's certainly been a lot of discussion about what meaningful consent looks like throughout the course of this study. We've heard today the witness talk about drivers in their current policies as a corporation under current legislation.

I want to state that it's my hope that we extend this investigation into what I consider to be the underlying deficits in Canadian privacy, transparency and accountability laws, deficits that have enabled this kind of collection in what I consider to be a surreptitious way and, as has been identified, the capitalization and commodification of data, big data in particular.

My question is that if this session of government was able to effectively modernize our privacy acts and legislation to bring big data under the purview of privacy, as I believe big data technology has certainly surpassed its current use, how would Telus adapt to include all data in their frameworks of meaningful consent?

Mrs. Pamela Snively: That's a challenging question without knowing what the changes would be.

I do want to make one thing clear, and it is that we have gone above and beyond the law. A lot of the things that we have been doing in our strong de-identification methodology, including our rigorous reviews of the purposes for which this data is used, the transparency on our website and the transparency specifically around Data for Good, are the types of things that would likely be in the new legislation.

● (1720)

Mr. Matthew Green: Mr. Chair, I'm going to ask one specific question, and hopefully the witness can provide the response back in writing.

We heard time and again about de-identified versus personal data. If we were to treat de-identified data as we did personal data and given its source, could the witness provide us, in writing, how they would go about providing meaningful consent to their clients when they're using data this way?

The Chair: You have a few moments to answer as well.

Mrs. Pamela Snively: I can take that away.

The Chair: All right. If that's sufficient, we'll look for a written response to that question.

We'll go now to Mr. Kurek for five minutes and we'll finish off with Ms. Saks.

Mr. Damien Kurek: Thank you very much, Mr. Chair, and again thank you to the witness for your testimony here today.

I hope we can get some more information about both the portal and the information that was provided to PHAC. In addition, as I've been considering your testimony, it would be very helpful and important for Canadians to be able to understand what the query-based system looks like and what types of queries could be asked.

Could I ask that this information be provided to the committee so that we can consider it as we are writing our report?

Mrs. Pamela Snively: Absolutely. I can take that back and discuss how to present that to you with my team.

Mr. Damien Kurek: Thank you very much.

I'd like to transition a bit, if I could. You referenced a number of times that Telus had spoken with the Privacy Commissioner. I'm wondering if you received an opinion from the Privacy Commissioner on the Telus Data for Good program. Was it just a discussion? Can you outline exactly what that interaction was?

Mrs. Pamela Snively: Thank you for the question.

Prior to launching Data for Good, as I indicated earlier, we designed our five commitments around the sharing of data and protecting privacy. We were trying to anticipate what our customers would be most concerned about if they were to hear about this and we were trying to address those concerns.

It was very much part of our transparency plan to publish these five commitments, as well as a description of the program and along with FAQs. We took the description of the program and the five commitments and sent those to the Privacy Commissioner. We asked for feedback on those, which they provided, and we incorporated that feedback.

Mr. Damien Kurek: I find it ironic that it appears that Telus went through more steps to protect its users' privacy than the Public Health Agency of Canada did, certainly in reference to the testimony that we received earlier.

When it comes to what the Public Health Agency of Canada did, were there frameworks or restrictions that would have ensured that this data was siloed or had a certain restricted level of use that wouldn't have gone beyond PHAC? Was there anything to ensure that queries and information that were sent to PHAC had to be managed carefully? When the data leaves Telus, what assurances were there that it wouldn't be shared with other agencies and departments of government, for example?

Mrs. Pamela Snively: It's very important to reiterate that these were not actual data sets that were provided to PHAC. We're talking about heat maps and derived data, so there were—

Mr. Damien Kurek: I understand that.

As the Public Health Agency of Canada was using your platform, dashboard and whatnot, were there assurances and requirements that PHAC would be the only agency allowed to use that, or were they given permission to share it more broadly?

Mrs. Pamela Snively: They were given permission to use it in accordance with the purposes of containing COVID. We were aware that they would be sharing it more broadly, sharing it wherever it could be used to serve that particular purpose, which was the containment of COVID-19 and to help fight the pandemic. That was the social purpose behind the program; if it was consistent with that social purpose, sharing was permissible.

● (1725)

Mr. Damien Kurek: With that in mind, I'm very curious as we look forward. There has been an RFP put out by the government asking for data related to the fight against COVID-19, but it also requested data for purposes beyond that. We've heard some testimony about what some of the challenges are around that, and this committee unanimously asked for there to be a pause on it until we have a better understanding as to what those are.

Are you aware of that RFP, and do you have any comments on it?

Mrs. Pamela Snively: I've heard about the RFP. I don't have any comments on it.

The Chair: With that, you're out of time.

Mr. Damien Kurek: Thank you very much.

The Chair: We'll go to Ms. Saks for the final five minutes.

Ms. Ya'ara Saks: It's been a long but very informative afternoon, and I want to thank our witness again for her very detailed explanation of the steps, processes, supervision and thought that went into constructing the Data for Good platform and its uses.

Telus's Data for Good platform is not only used by PHAC; it's used by university researchers. It's almost like a library, in some ways, with a lot of supervision and guardrails. Would you agree?

Mrs. Pamela Snively: It's with a lot of guardrails and supervision, yes. The idea is to support evidence-based decisions.

Ms. Ya'ara Saks: Absolutely.

I'll phrase it this way. From its inception, you took a very deliberate approach in designing the Data for Good platform. In the end, you won awards and you've received accolades from Dr. Ann Cavoukian.

Could you talk about the guidelines or metrics that you used? In his testimony, the commissioner talked about frameworks that he outlined in relation to the COVID Alert app. I'm not sure if they are public or not public. Based on your previous comments, I'm not sure they are.

We talked about privacy by design, but were there other frameworks, either from the Privacy Commissioner or the Ontario privacy commissioner, that helped guide and structure the process for design and how you use it now?

Mrs. Pamela Snively: In terms of specific frameworks, as I said earlier, we did work with experts from across the country as well as even outside the country to look at the best strategies and techniques for strong de-identification.

There are a number of different strategies to approach de-identification. We employed more than one and took a bit of a belt-and-suspenders approach, but is there an actual standard of taking these 25 steps and you will have de-identified data? That doesn't exist. It is contextual, and it's more complex than that.

We have worked with all the leading experts on how to develop frameworks that are as robust as possible.

Ms. Ya'ara Saks: Thank you.

Mr. Chair, I'm going to be sharing my time with my colleague Ms. Khalid, so I will pass the floor to her.

Ms. Iqra Khalid: Thanks very much.

How many minutes do I have, Mr. Chair?

The Chair: You have a little over two minutes.

Ms. Iqra Khalid: Thank you very much for your testimony and for answering our questions. It's much appreciated.

We have been asking a lot of questions around informed consent for the use of Canadians' data. Perhaps I want to take a step back and put it into more layman's terms that Canadians can understand.

Let's say, for example, that somebody signs a petition that is being circulated by an MP who is running to be the leader of a party. Would that MP need informed consent to then later use that data for other purposes, as opposed to just the reason this person signed that petition? If that data was used for other matters, for data mining or what have you, would there be an obligation on that organization to seek that informed consent, do you think?

Mrs. Pamela Snively: I think that's a really interesting question. It's a great question, because the analogy might be to say that there are 3,000 people who signed the petition to support a particular MP, and the MP makes the conclusion that 3,000 people in the country support him or her. That conclusion is the type of insight we're talking about.

If the MP goes says, “I have 3,000 people supporting me, and that's why I think I should be able to do this, raise this much money or do these other things” and if that's not what their original intention was when they signed up and they were just signing it for some other reason, then we're in the same boat.

Clearly that's not the idea here. We're talking about aggregated concepts, of patterns and trends, and nobody would expect that the MP would go back and get consent from everyone for every conversation that he or she has about that 3,000 number.

● (1730)

Ms. Iqra Khalid: Thank you so much for that.

Do you have any recommendations with respect to strengthening government policy on how companies, private or public, collect, store and use data? I mean specifically with respect to informed consent and how the framework is in our government.

The Chair: We're going to have to wrap it up. You are over time now.

We'll have a quick comment or response from the witness, and then we're going to have to wrap it up.

Mrs. Pamela Snively: We have been actively participating in any consultations that the government has been holding on how best to improve our privacy legislation, so I will leave it at that.

The Chair: Thank you very much. That will conclude panel two.

There were several questions that require written responses, and I think there was an undertaking from the witness to provide that in some cases. If you are able to do so, please do so as soon as possible.

With that, this meeting is adjourned.