HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

44th PARLIAMENT, 1st SESSION

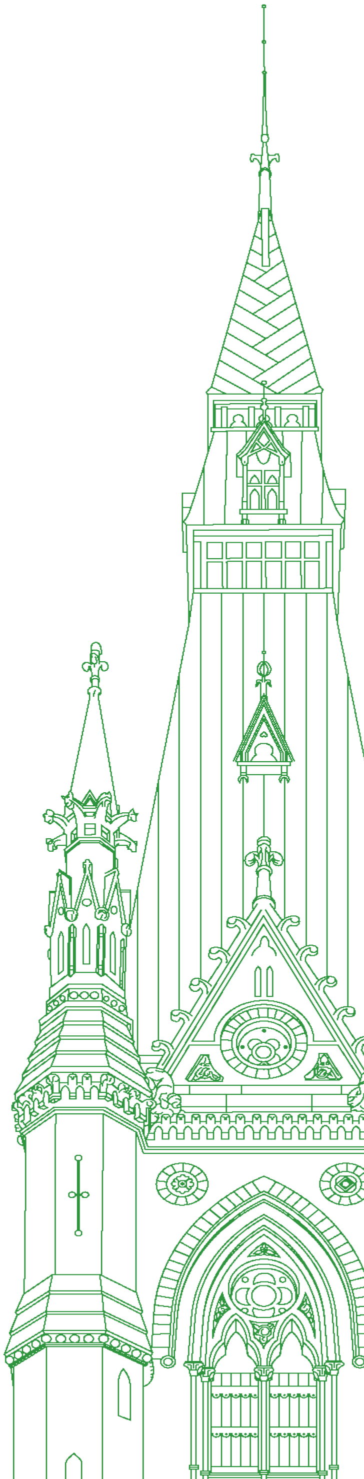
Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 005

PUBLIC PART ONLY - PARTIE PUBLIQUE SEULEMENT

Monday, February 7, 2022



Chair: Mr. Pat Kelly

Standing Committee on Access to Information, Privacy and Ethics

Monday, February 7, 2022

● (1100)

[*English*]

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

[*Translation*]

Welcome to meeting number 5 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 commenced its study on collection and use of mobility data by the Government of Canada.

[*English*]

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

I would like to take this opportunity to remind all participants of this meeting that screenshots or taking photos of your screen is not permitted.

Given the ongoing pandemic situation and in light of recommendations from health authorities, as well as the directive from the Board of Internal Economy on October 19, 2021, to remain healthy and safe, all those attending in person are to maintain a two-metre physical distance and must wear a non-medical mask when circulating in the room. It's highly recommended that the mask be worn at all times, including when seated. When you are speaking, though, it's sometimes easier to remove it. I will remove my mask when I'm speaking. Persons also must maintain proper hand hygiene by using the provided hand sanitizer at the room entrance.

As the chair, I will be enforcing these measures for the duration of the meeting, and I thank members in advance for their co-operation.

To ensure an orderly meeting, I would like to outline a few rules to follow.

Members and witnesses may speak in the official language of their choice. Interpretation services are available for this meeting. You have the choice, at the bottom of your screen, of floor, English or French. If interpretation is lost, please inform me immediately and we will ensure interpretation is properly restored before resuming the proceedings. The “raise hand” feature at the bottom of the screen can be used at any time if you wish to speak or alert the chair.

For members participating in person, proceed as you usually would when in a committee room. Keep in mind the Board of Internal Economy's guidelines for mask use and health protocols.

Before speaking, please wait until I recognize you by name. If you are on the video conference, please click on the microphone icon to unmute yourself. For those in the room, your microphone will be controlled as normal by the proceedings and verification officer. When speaking, please speak slowly and clearly. When you are not speaking, your mike should be on mute.

As a reminder, all comments by members and witnesses should be addressed through the chair.

With regard to a speaking list, the committee clerk and I will do the best we can to maintain a consolidated order of speaking for all members, whether they are participating virtually or in person.

I would like to welcome our witnesses. From the Office of the Privacy Commissioner of Canada, we have Daniel Therrien and Martyn Turcotte, who is director of the technology analysis directorate.

Before I turn it over to the commissioner for his opening statement, I will say that I am going to devote part of the time in the second panel to committee business. This was requested by a member of the committee, and I think it's time we had a discussion of committee business. I will aim, if we can make everything run on time.... Hopefully we can have up to half an hour for committee business, but that will depend, in part, on keeping on schedule.

With that, I will turn it over to you, Commissioner. Thank you very much for appearing. You have five minutes for an opening statement.

● (1105)

[*Translation*]

Mr. Daniel Therrien (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): Thank you very much, Mr. Chair.

Thank you for the invitation to appear in connection with your important study.

Early in the pandemic, the Office of the Privacy Commissioner of Canada recognized that data can serve the public interest, such as protecting public health. To that end, we published a framework for how to achieve this while respecting privacy, a key point of which was to use de-identified or aggregated data wherever possible.

Our framework cautioned that institutions should be aware there is always a risk of re-identification. Given this risk, our framework was explicit that there needs to be technical and other means implemented to protect the information. In principle, then, the use of de-identified or aggregated data for public health purposes is consistent with our framework, provided appropriate technical standards are used.

Since the beginning of the pandemic, we have had regular meetings with the Public Health Agency of Canada on COVID-related initiatives. We welcome these interactions.

In the case of the government's use of mobility data, we were informed of their intent to use data in a de-identified and aggregated way. We offered to review the technical means used to de-identify data and to provide advice, but the government relied on other experts to that end, which is its prerogative.

Now that we have received complaints, we will investigate and turn our attention to the means chosen for de-identification and whether they were appropriate to safeguard against re-identification. Since this is under investigation, we will not be able to provide you with advice on this aspect of your study.

[*English*]

I would now like to offer the following observations on how this case is only one example of much more widespread practices in the public and private sectors and why, in my view [*Technical difficulty—Editor*] the urgent need for law reform. I also wish to suggest issues that you may want to consider during your study.

Organizations in both the public and private sectors constantly reuse data to new ends. This practice raises legitimate concerns by consumers, particularly when their personal information is used without their knowledge for purposes other than those they expected. Is the solution to ensure meaningful consent is obtained for all such cases? I think this is neither realistic nor reasonable, as this case illustrates.

The solution, in my view, would be to authorize the use of personal data for socially beneficial purposes and legitimate commercial interests within a rights-based law that acknowledges the nature and value of privacy as a human right so as to give privacy its appropriate weight in any balancing exercise.

The government argues that its use of mobility data did not engage the Privacy Act: in other words, that the act does not apply. Oddly, if the data was properly anonymized and aggregated—a fact that your committee and our office will separately investigate—that conclusion is likely legally correct, so the first question you should consider is whether the data, indeed, was properly de-identified and aggregated.

Even if it was, I would suggest that the second issue is whether it is good legislative policy that de-identified information falls outside the reach of privacy laws. We think removing de-identified information from the reach of these laws would bring very significant risks and is not good policy.

There is then the question of transparency and consent. Did the government or its private-sector partners adequately inform users that their mobility data would be used for public health purposes? While there is a reference to the “data for good” program somewhere in Telus's privacy policies, and while the government does make an effort to inform citizens of its use of mobility data on its COVIDTrends web page, I do not think anyone would seriously argue that most users knew how their data would be used.

Does that matter? That, I suggest, is another question you should consider. There's no question that transparency is important to enhance trust, and the government could likely have been more proactive in informing Canadians about its program, but should programs like this require meaningful consent?

● (1110)

As I mentioned earlier, I believe that due to the limitations of the consent model in protecting privacy, a more appropriate policy would be to authorize the use of personal information for legitimate commercial interests and the public good within a rights-based law. That law should be enforced by the OPC, an independent regulator, to which would be conferred the requisite powers and resources to protect Canadians.

The Chair: I apologize for not giving you a warning, but you are pretty much out of time.

Mr. Daniel Therrien: I'm happy to take questions.

The Chair: With that, I will go to Mr. Brassard for six minutes.

Mr. John Brassard (Barrie—Innisfil, CPC): Thank you, Mr. Chair.

My preference would have been for Mr. Therrien to continue, because he certainly is the expert in this field and has a lot to say.

Mr. Therrien, I want to thank you for being here today. I believe this is an important study. It's important because Canadians are seized with the issue of privacy. I think what it also does, Mr. Therrien, is allow this committee to look at the very issues that you've highlighted in your opening statement and that you've written to other privacy commissioners about. You've written to the government about protecting privacy in the pandemic.

What I really want to clarify has to do with the consultation of your office. I happen to believe, and I believe many Canadians do as well, that if it is not the Privacy Commissioner of Canada's office that needs to be consulted, then who else needs to be consulted? In other words, you are the standard by which privacy is met in this country, and yet we hear conflicting reports that you were consulted or you weren't consulted.

PHAC went out and advised that they were looking at other security experts and privacy experts. What would those other security and privacy experts offer the government that the Privacy Commissioner of Canada and his office could not?

Mr. Daniel Therrien: On the facts of whether we were consulted or informed, and what was the tenor of these discussions, we were informed by PHAC and a group within the innovation department that the government wanted to use de-identified information for the purposes outlined: i.e., use mobility data to determine trends in mobility for public health purposes.

We were informed of this as part of regular meetings with government agencies on any number of COVID alert issues. At that time, we were heavily involved in the COVID Alert app, among other things, so we were informed of this particular project.

We offered to provide advice on the adequacy of safeguards to ensure that the data was properly de-identified, and the government decided to rely on others. That's their prerogative.

Mr. John Brassard: Is that normal, Mr. Therrien? It's their prerogative, but is it normal for them to seek outside security and privacy expert advice when, in fact, it's your office that's charged with protecting and providing that advice to the government on privacy rights? I find it highly unusual that they would do that.

Mr. Daniel Therrien: We offered to provide advice. Is it normal that we not intervene in every case? I think the reality is that we, as an office, cannot be involved in pre-authorizing or reviewing every case of data collection or disclosure that occurs in Canada. We give general advice that we hope is followed. We investigate complaints.

I think that in the new law our office should have greater powers to proactively audit the practices of governments and the private sector, but unfortunately it is just not realistic to expect that we will pre-approve every use or disclosure of data in this country. At the end of the day, it is to the benefit of Canada that data is shared, obviously for good reasons—for legitimate commercial interests, for the public good, and not for illegitimate surveillance as we've seen in certain cases.

Because these practices occur all the time, we just cannot be there all the time.

● (1115)

Mr. John Brassard: Right, but it is reasonable to expect, on behalf of Canadians, that going outside to other privacy and security experts doesn't guarantee that the government or, in this case, the telecom communication companies are following the privacy laws.

Would that be an issue of concern for you, that going outside of what is the de facto expert in this country would...? It's almost like finding a lawyer who agrees with you. One doesn't, the other one doesn't, but then you go to another lawyer and they say, “Yes, okay, you are following the law”, but it actually doesn't make it so. Does that concern you?

Mr. Daniel Therrien: We're not the only experts. Expertise is not spread evenly among all institutions, but here, we're dealing with the Government of Canada, which has experts, and with large telecom companies that also have experts. We offered our expertise. It was declined. It is what it is.

Mr. John Brassard: Thank you, Mr. Therrien.

You mentioned consent, and the importance of consent. One could argue easily that Telus and its “data for good” offers an opt-out provision. However, in most cases, and we've heard in testimony that in some cases....

Mr. Chair, am I just about out of time?

The Chair: You're just about out of time.

Mr. John Brassard: It's just the importance of informed consent as it relates to data gathering.

Mr. Daniel Therrien: Again, consent is not a silver bullet or a solution for all cases. There's no question here that, as I said in my statement, most Canadians whose data was used did not know their data was used. The parties, both the government and the private sector, could have done more to inform users that their data was used for these purposes.

Mr. John Brassard: Thank you.

The Chair: Thank you.

We'll go to Mr. Fergus, for six minutes.

[*Translation*]

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

I'd also like to thank Mr. Therrien for his testimony today and for being available to offer his comments and expertise.

We are very grateful for your work, Mr. Therrien.

The committee decided to conduct a study “of the Public Health Agency of Canada collecting, using or possessing Canadians' private cellphone data”. A spokesperson for the Public Health Agency of Canada has clarified that only de-identified or aggregated data are used.

Mr. Therrien, based on your assessment of the communications your office has had with PHAC, can you tell us whether, *prima facie*, the government did receive de-identified or aggregated data?

Mr. Daniel Therrien: I cannot, because that is the subject of the investigation we are going to have to conduct as a result of the formal complaints we have received under the law.

What I can say is that we have had discussions with PHAC. They informed us, again, that they intended to use de-identified or aggregated data for public purposes, such as public health. This is consistent with our understanding of privacy principles.

As to whether the data was de-identified properly, we don't know yet. We will investigate.

● (1120)

Hon. Greg Fergus: Mr. Therrien, there were no red flags in April 2020 when you started those discussions, were there? I would imagine it was because PHAC was doing its job and asking to receive de-identified data in accordance with the important principles that your office and the government established, right?

Mr. Daniel Therrien: The information provided to us was, in principle, consistent with the framework we had established. We offered to go under the hood to determine if the data had indeed been de-identified properly, but the government declined that offer. In terms of principles, we saw no problem. As what happened in practice, we will investigate. I have no reason to believe that things were done correctly or, conversely, inappropriately. That will be investigated.

Hon. Greg Fergus: Mr. Therrien, apparently the data was published transparently. Again, I ask: Do you have any reason to be concerned that the published data has not been adequately de-identified?

Mr. Daniel Therrien: That's what we will be investigating. I cannot comment on that at this time.

Hon. Greg Fergus: Has this data been in the public domain for some time, Mr. Therrien?

Mr. Daniel Therrien: Yes, it was published several months ago.

Hon. Greg Fergus: In your opinion, how long will it take your office to complete a proper assessment and determine whether or not the government has been able to protect Canadians' personal information?

Mr. Daniel Therrien: We received complaints at the very end of 2021, about two months ago. We referred questions to the appropriate departments a few weeks ago, but we're still waiting for their responses. I wish I could tell you that we will be able to conclude the investigation while your study is under way, but I don't think we possibly can.

As I told you, we still haven't received a response from the departments. I don't mean to imply that the responses are late. It's just the normal course of events. In the months following the completion of your study, we will be able to close the investigation.

Hon. Greg Fergus: Mr. Therrien, I want to say again that I greatly appreciate your work and that of your office. I certainly respect your professionalism. Having said that, if it takes several months to determine whether data has been de-identified, in your opinion, does that explain why the government decided to bring in other experts in the field?

The pandemic had an impact on everyone and the government needed to come to a conclusion. This was an unusual situation.

[*English*]

The Chair: Can I get you to wrap up, Greg? We're out of time.

[*Translation*]

Hon. Greg Fergus: Perhaps Mr. Therrien could answer my question in writing.

[*English*]

The Chair: Yes, I'll let him answer, but you're out of time.

[*Translation*]

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

[*English*]

The Chair: Please give a brief answer.

[*Translation*]

Mr. Daniel Therrien: In a formal investigation, if we had been consulted, we could have made conclusions based on information that, I would remind you, the government still hasn't provided to us. In addition, in an investigation, you have to hear from both the complainant and the respondents, which draws out the investigation.

[*English*]

The Chair: Thank you.

[*Translation*]

Mr. Villemure, you have six minutes.

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

Had the Privacy Commissioner been given the choice, he would have stepped in? Am I right?

● (1125)

Mr. Daniel Therrien: As I mentioned earlier, we offered our advice, but the government decided to seek it elsewhere.

Mr. René Villemure: Very well, thank you.

In this whole thing, I'm much more interested in where the data came from than where it ended up. You stated earlier that it was virtually impossible to get informed consent from the people whose data was used.

In your view, can presumed consent replace informed consent? I don't mean under the law, I mean proper consent.

Mr. Daniel Therrien: In this case, I'm going on the premise that consent has a role to play in protecting privacy, but it's unrealistic in today's modern world to expect that all commercial or government use of a customer's data should be subject to consent. That brings us to the concept of consent that is oftentimes implied.

In the event of implied consent, the legal principle is that properly de-identified data, being something that is entirely possible to do, is simply not personal information under current public sector law. So the government can collect and use it as it sees fit, without having to protect privacy. This is entirely possible, even though we haven't yet reached a conclusion.

Therefore, the rule that seems to apply in this case is that, if properly de-identified, data is not personal information and consent is not required.

That's one reason we recommend that, even if data is de-identified, the law should be amended to remain subject to the Privacy Act, so that certain principles apply, even to de-identified data.

Mr. René Villemure: All right, thank you.

Do you believe the average cellphone user understands that their data can be used for purposes other than improving networks, for example? I'm not talking about the user knowing this, but understanding that aspect of it.

Mr. Daniel Therrien: No. People aren't fully aware of certain uses.

Mr. René Villemure: Telus customers could choose to opt out of giving consent. All they had to do was go to the Telus website and do it. Again, they had to know about and understand that.

Should it be made clearer to customers that they are free to opt out?

Mr. Daniel Therrien: That essentially amounts to saying that cellphone users were unaware of the practice and therefore were unable to opt out. People can't withdraw consent when they don't know it's an option.

As I was saying, in my opinion, more steps should have been taken by Telus and the government to inform Canadians of how their data was being used.

Mr. René Villemure: Should this be part of the proposed review of the legislation?

Mr. Daniel Therrien: The principle of transparency should definitely be included in the Privacy Act. There should be greater transparency.

Mr. René Villemure: Do you know of any countries around the world that have transparency principles in place and do a better job enforcing them?

Mr. Daniel Therrien: I would say that in Europe, the laws are certainly more stringent. That said, we can provide you with a more detailed answer in writing, if you wish.

Mr. René Villemure: Thank you. That would be extremely fascinating.

In other words, even if the letter of the law or the regulations allowed Telus to make such use of customer data, the user would not understand it.

Mr. Daniel Therrien: That's right.

As I said in my remarks, I don't think the ultimate solution is simply greater transparency and explicit consent, given that data is used in an extremely wide range of ways, sometimes for good reasons, sometimes for bad.

Therefore, you need objective criteria, covering things like legitimate commercial use and using data to serve the public good, that a regulatory agency would enforce. Consent is important, but a regulatory agency also needs to play a role in properly protecting Canadians, given the complexity of how their data is being used.

● (1130)

[*English*]

The Chair: Monsieur Villemure, I'm afraid you're out of time.

[*Translation*]

Mr. René Villemure: Okay.

[*English*]

The Chair: Now we will go to Mr. Green for six minutes.

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

Through you, Mr. Chair, to Mr. Therrien, I just want to introduce myself as the honourable member representing Hamilton Centre. I only have about six minutes, so I'm going to put some questions to you in a rather rapid way. I ask for your forgiveness if it seems as though I might move you along on a particular question to get to the next one.

I share the concern of members around the table about the discrepancies regarding what we heard in our February 3 meeting, last week, what the Public Health Agency of Canada presented, along with the minister, in terms of what the engagement was with your office. I've heard you now say that you were informed. I'll share with you that in the previous meetings there was the implication that there was a collaboration or a consultation.

I want to be clear on the difference between having your office be informed of something on an ongoing basis versus what it might look like if you were actually engaged in consulting with the department on matters of privacy. In a brief description, can you just lay out the difference between those two things?

Mr. Daniel Therrien: When we are in engagement, whether with a public sector institution or a commercial organization, we receive detailed information about the information flows and the protections given to information, so as to be able to say not only that in principle privacy is respected, but that in fact we have actually looked “under the hood”—to use an expression—to ensure that indeed the personal information of Canadians has been protected.

Here, we did not have a chance to look under the hood.

Mr. Matthew Green: I will take it that it will likely be part of the ongoing investigations that you have, based on complaints, to look under the hood in terms of the framework that you put forward, which was explicit in terms of the need for technical and other means to be implemented to protect the information. Is that correct?

Mr. Daniel Therrien: Indeed, and the law, of course.... We'll look at our framework and the law.

Mr. Matthew Green: Can you be more explicit about your framework? Without getting into the deep technical weeds, are all ministries, all departments within the federal government, aware of your framework, given the very sensitive nature of this time during COVID and the sharing of information and the effects on privacy?

Mr. Daniel Therrien: The framework was distributed to all departments and we have certainly had discussions with several of them, so my sense is that indeed the framework is known within the federal government.

Mr. Matthew Green: Are other departments actively engaging you in a more one-to-one consultative process?

Mr. Daniel Therrien: There are a number of departments, maybe not a majority, but Health Canada certainly.... The Public Health Agency is the agency that consults us the most during the pandemic. One would expect that. A number of other departments—

Mr. Matthew Green: Except for this. Just to be clear, when you offered to review their technical means to use de-identified data and provide advice, PHAC declined. Is that correct?

Mr. Daniel Therrien: Yes. They informed us of the program but declined our offer to look under the hood.

Mr. Matthew Green: I'm going to switch gears now. Something that I'm very interested in is your identification of the urgent need for law reform. I couldn't agree more. Rather than have this study be a giant fault-finding mission, my hope is that facts could be presented to this committee that will become part of the recommendations of this committee to ultimately reform the gap between...what you've identified as legitimate uses for commercial interests and social good.

In the remainder of this time, could you present to this committee some of the points of urgent law reform that you would be exploring and recommending, in a preliminary way?

● (1135)

Mr. Daniel Therrien: I would start with the fact that data, including personal data, is necessary for economic development, economic growth and for the social good. We're not saying that data should not be used. It is the way of the 21st century. It is the way of the future.

However, the fact that data can be used for good, of course, does not mean that it is always so. We have seen many cases over the years of data used against the interests of individuals. Think of Cambridge Analytica, for instance, and the link to democracy.

The framework needs to allow for flexibility and innovation in the use of data for legitimate commercial interests and the public good, but within a framework that protects privacy as a human right, enforced by a regulator who can audit or investigate to ensure that, in individual circumstances, the data indeed was used correctly or not, and when not, there should be consequential penalties for players, corporations, that have violated the law.

Essentially, that is the framework that we have.

Mr. Matthew Green: I have a quick question.

The Chair: You can ask a quick one.

Mr. Matthew Green: You referenced Cambridge Analytica. That to me brings up Facebook. We look right now at Europe's restrictions on Meta's use of U.S. servers under a so-called “privacy shield”. Is there a need for us in Canada to have our own privacy shield as it relates to international servers?

The Chair: Give a very quick answer, please.

Mr. Daniel Therrien: I would say simply this: not necessarily a privacy shield, but laws need to be interoperable between countries and within Canada.

Mr. Matthew Green: Thank you so much for that, Mr. Chair.

The Chair: With that, we go to the next round.

We will begin with five-minute slots, starting with Mr. Kurek.

Mr. Damien Kurek (Battle River—Crowfoot, CPC): Thank you very much, Commissioner. I appreciate your being here to join us today and share what I think are very valuable insights into this important subject. There seems to be a key metric here, the de-identified and aggregated data really being the capstone of what we're trying to get to the bottom of.

Commissioner, the minister this past week said that they had biweekly meetings with the Privacy Commissioner's office. I believe that's what the minister said. Did the subject of this data and what “de-identified” and “aggregated” actually meant come up during any of those meetings?

Mr. Daniel Therrien: It is true that we have had meetings roughly every two weeks with the Public Health Agency on various measures related to COVID and their impact on privacy. In the period in question—it was in the early days of the pandemic, March and April 2020—there were a lot of subjects being discussed, including the COVID Alert app. We were informed of the particular program that you are currently reviewing on the basis that the government felt that it was obtaining anonymized and aggregated data. It's on that basis that we offered to provide advice. It was declined. We don't have a role to pre-authorize every government initiative, so we left it at that.

Mr. Damien Kurek: That you for that, Commissioner.

When it comes to de-identified and aggregated data, what are some of the risks associated with that? We have yet to hear or see exactly what that data looks like. Could you describe some of the risks that could be associated with that, and maybe provide a definition of what that means, especially in the context of something like this? We're talking about the data of what has been suggested—although there are varying accounts—to be 33 million mobility users' information.

Mr. Daniel Therrien: Data is de-identified because it was originally identifiable. We start with personal information. There's no question that a telco like Telus had information about its users' mobility data, because it is necessary for Telus to obtain that information in order to deliver the service that they offer to their clients. You start with what is clearly personal information about users of telecom services. De-identification means that you transform that personal information through technological means—which I'll ask my colleague Martyn Turcotte to describe, if we have the time—to reduce the risk that individuals will be identified.

What needs to be understood is that, even when data is properly de-identified, there is always a risk of re-identification through data matching, through all kinds of possibilities. That is why, given the risk of re-identification in every case, we are suggesting that it is not good policy under the current law to treat de-identified information outside the scope of the Privacy Act.

● (1140)

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

I'm almost out of time, but I do want to ask one more quick question.

Was your office consulted on the tender that has been put on hold to continue this practice going forward, in what the explanation suggests is not only for the COVID-19 pandemic but possibly beyond that? Has your office been consulted and, if so, what does that look like?

Mr. Daniel Therrien: We were not consulted. We asked for information in late 2021 about this process and were given some information, but I would not say that this constituted a consultation. We were informed.

Mr. Damien Kurek: Thank you very much, Commissioner. I appreciate that.

The Chair: Thank you.

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

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

I want to thank Mr. Therrien for joining us today and answering all these very important questions. I agree with my colleagues.

I want to go back to your opening statement when you were talking about transparency and consent. You wondered whether it was obvious to Canadians that their data was being used this way.

I believe it was as early as 2020 that there was a news release from the Prime Minister's Office about the fact that Public Health was going to start using de-identified mobility data to help with its fight against COVID-19. I wasn't part of the government at the time, but I certainly remember hearing about this happening. I remember the tweets regularly from our chief public health officer, Theresa Tam, talking about this data and what it meant. We knew, for example, if public health measures were being followed because the mobility data showed that people weren't moving as much, and then we could find trends because of the mobility data. I saw regularly information coming from the government about how this data was being used, and I didn't see any concern about it until the opposition brought it up a couple of months ago.

When you say that the government could have been more proactive in its communications about the use of mobility data, how exactly would you suggest that could have been done better?

Mr. Daniel Therrien: Transparency is tough. As I said in my opening remarks, the government has a COVIDTrends web page that does a fairly good job of explaining to Canadians that their mobility data is used. You don't need to go through a 60-page privacy policy to find that out, but in order to get to that page, you need to know that the program exists and that there is something called COVIDTrends. Once you're there, it does an okay job of transparency.

Beyond the web page, I think you're right to ask how the government can be proactive. It would be through communication strategies and news conferences that are given by PHAC and others, for instance, so that would be proactivity.

The bottom line for me is that I highly doubt that the majority of users of mobility services knew that their data was collected, despite the efforts made by the government.

Transparency is important, but it is not sufficient to ensure that data is properly regulated. That's why I said that in addition to transparency, in addition to consent, there needs to be an authority for the regulator, as we're doing now, to investigate a situation like this to ensure that privacy is protected.

● (1145)

Ms. Lisa Hepfner: Thank you.

When you say that most users didn't know that their data was being used in this way, what are you basing that on? Do you think people don't know that their data is being used, or that mobility data is being used?

Mr. Daniel Therrien: I think this is the case generally, that people do not have an awareness or a consciousness of the many ways in which their data is used. Hopefully a cellphone user would know that their data is collected by Telus and maybe by a few companies around Telus, but they would not know generally that their data is used for a program like this. I think that's pretty clear.

When we speak to Canadians, their premise is that their data is used for the purposes for which they provided it to the company or the department in question, and maybe a few around, but not for any and all purposes that we see nowadays. That's not the expectation of people. I think that's pretty clear.

The Chair: Thank you.

I'm afraid we're out of time.

Ms. Lisa Hepfner: We're out of time, okay.

The Chair: Now for two and a half minutes, we have Mr. Villemure.

[*Translation*]

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

Thank you, Commissioner, for your candour and the detail you provided.

I imagine that the Office of the Privacy Commissioner was created to maintain public trust in privacy. You spoke of trust in your remarks, and we all know that when trust is not there, mistrust sets in, and then eventually gives way to distrust.

Do you feel that these incidents—I don't want to use the word “scandals”—around privacy erode public trust in authorities, in general?

Mr. Daniel Therrien: Yes, and the government introduced legislation in the previous Parliament precisely to improve Canadians' confidence in how their data was being used.

Mr. René Villemure: Well, as we've seen, the law was a bit lacking.

We were discussing the European regulations a little earlier. I believe you referred to the European Union's general data protection regulation.

Mr. Daniel Therrien: Yes.

Mr. René Villemure: What might we “import” from that regulation to our legislation?

Mr. Daniel Therrien: I am going to somewhat reiterate the answer I gave earlier to Mr. Green. In our annual reports, we explained that in general terms.

I will go back to the trust part of your question. Consent and control are ways to ensure that Canadians have trust. However, I don't believe that Canadians or users in general around the world want to have to consent or not consent to the myriad uses of their data. Canadians want to be able to use modern technology with the assurance that their rights will not be violated. This depends in part on individual consent, but more importantly, it depends on Canadians being assured that someone is there to protect their interests. However, that individual must have the powers to do that.

Mr. René Villemure: So basically, Canadians need to be able to understand that and place their trust in you.

● (1150)

Mr. Daniel Therrien: Yes. On the one hand, they must exercise their consent and, on the other, they must place their trust in someone else.

Mr. René Villemure: Thank you.

[*English*]

The Chair: Thank you.

Now we have two and a half minutes for Mr. Green.

Mr. Matthew Green: Thank you.

There are some very interesting things here, particularly around the idea of a rights-based law.

It was noted in the opening remarks by Mr. Therrien that Justice Canada outlined a similar approach in its proposals for the Privacy Act modernization. He went on to state that some would prefer that de-identified information be removed from the reach of privacy laws. In Mr. Therrien's opinion, who would those people be who would seek to benefit from de-identified information being removed from the reach of privacy laws?

Mr. Daniel Therrien: Obviously, that would be people who want to innovate with as few limitations or restrictions as possible, like the idea that de-identified information would not be subject to privacy protection.

Mr. Matthew Green: Right off the bat, to be de-identified, at its source it has to be identified.

Could Mr. Therrien perhaps comment on whether or not there could have been...? Maybe that's too close to the investigation; I'll stay away from that.

He mentioned the idea of greater power to proactively audit the government and the private sector. I want him to reflect on that, expand on what that might look like and also perhaps add in this idea of defining what legitimate commercial interests are. I will share with you that I have a significant concern about the commodification of private information and the way it's used in big data.

Mr. Daniel Therrien: On the question of proactive verifications, I'll say this. The idea is not to be a thorn in the side of governments or companies that want to innovate responsibly. The point is that data flows are so complex and business models are so complex that individual Canadians are not well placed when identifying violations of private [*Technical difficulty—Editor*] and that a body like the OPC is better placed, not to go after thousands of companies a year, but on a risk basis to, again, go under the hood in a number of places where we think there might be risks so that we can either reassure Canadians that the law has been respected or intervene and sanction companies that have not complied with the law, so that confidence in the system is enhanced.

The Chair: Thank you.

Mr. Matthew Green: Mr. Chair, could I ask—

The Chair: I'm afraid you're out of time, Mr. Green.

Mr. Matthew Green: Just as a point of order, related to information that he had talked about, can we request, through you, that he provide in writing the explicit framework that he talked about?

The Chair: I think you just have.

Again, Mr. Green, I know that you're a big fan of only using—

Mr. Matthew Green: Get it in writing.

The Chair: —a point of order when there is actually a deviance from the regular practice or rule of the committee. Thank you, Mr. Green.

We will go to Mr. Brassard. I understand that he will begin and then perhaps split his five minutes.

Go ahead, Mr. Brassard.

Mr. John Brassard: Thank you, Mr. Chair.

Mr. Green, that was a proper point of order, by the way.

Mr. Therrien, first of all, you have given us a lot to consider today. I want to thank you for your frankness.

I want to talk about data that's properly de-identified. You said it's always at risk through data matching. We know that through this process, or we've learned that through this process.... Telus collected the data. It was passed on to a secondary source called BlueDot, whose business is presumably to take that data, assess it and provide guidance to PHAC, which eventually became the customer.

What is the risk of data being de-identified by a company whose business it is to deal with this type of scenario? Just talk about the risk, if you will.

Mr. Daniel Therrien: I would not go to the motivation of a company. I would go to what safeguards we're applying.

Mr. John Brassard: That's where I was going with this.

Mr. Daniel Therrien: That is what we would investigate.

Mr. John Brassard: Right. We have heard from security experts and privacy experts publicly—we haven't heard it at the committee, at this point—that those appropriate safeguards and protocols have to be put in place at the source. If they are not, then there is a significant risk of reidentifying that information.

Mr. Daniel Therrien: Mr. Turcotte, you may want to answer this one.

● (1155)

[*Translation*]

Mr. Martyn Turcotte (Director, Technology Analysis Directorate, Office of the Privacy Commissioner of Canada): Yes, Commissioner.

I will try to speak slowly, because I believe I'm having microphone issues.

When we talk about the risk of re-identification—

[*English*]

The Chair: Excuse me. I have to stop you, Mr. Turcotte. The interpreters are unable to interpret. I understand that you don't necessarily have the ideal headset for this.

I will maybe throw the question back to Commissioner Therrien to answer.

Mr. Daniel Therrien: We can answer in writing, but I think that Mr. [*Technical difficulty—Editor*]. He would also be well placed. Otherwise, we would be happy to answer in writing.

The Chair: With that, I think we're going to switch to Mr. Patzer.

You have two and a half minutes.

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

Mr. Therrien, I think Canadians at large were quite alarmed and surprised to learn that, as I think one article I read said, 33 million users had their data accessed by PHAC. It begs the question, how many other departments out there are accessing people's personal information within the federal government?

Mr. Daniel Therrien: What we have seen in the pandemic in particular is that governments, not only the Government of Canada but governments writ large, call on the private sector to develop digital programs in order to deliver services. That's not necessarily a bad thing, but what we see is that there is an increasing interaction between the public and private sectors in terms of the management of data.

Again, that's not a bad thing. It needs to be properly regulated according to known criteria, and be the subject of investigation when the case arises, but there are certainly other departments that do this.

Mr. Jeremy Patzer: Yes. I think the general concern, though, is that the government is taking people's personal data, but then it could potentially use it against them. Is that a concern? Are there any safeguards to prevent that from happening?

Mr. Daniel Therrien: If we're dealing with personal information collected by the federal government, the Privacy Act does offer some protections. It's a badly outdated law, about 40 years old, but it would be an exaggeration to say that there are no protections.

Mr. Jeremy Patzer: Yes. I think that's definitely problematic.

My last question goes back to when you appeared in 2020 before the industry committee, which I was a member of at the time. You indicated that when properly designed, tracing applications could achieve both public health objectives and the protection of rights simultaneously. I remember that at the time you had some concerns about that, because the government hadn't actually consulted you at that point in time. How were those concerns addressed, and what has been done to prevent that?

Mr. Daniel Therrien: Is your question about COVID Alert?

Mr. Jeremy Patzer: Yes.

Mr. Daniel Therrien: We were heavily consulted on COVID Alert, and I was able to say that the privacy protections for that particular application were actually quite high.

The Chair: Thank you.

Our last questioner will be Mr. Bains for a five-minute round.

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

Thank you to our witnesses for joining us today.

I know a lot of questions have been asked. You talked about how you highly doubt people know whether their data is protected or unprotected. Last week I talked about something similar.

I look at a number of apps that people are using across the country, everything from Google Maps to other apps that people have on their phones. It's probably in the hundreds. Typically, the app will ask you for access to your information and access to your camera. You said that something needs to be done to strengthen this protection. Is that something that you feel should be included in this feature?

● (1200)

Mr. Daniel Therrien: I'll distinguish two things. I heard you say—or perhaps I misunderstood—that there's a question of knowledge or awareness by Canadians, and a question of protection. As to whether the data of Canadians was adequately protected, that is the subject of our investigation, so I'm not saying it was protected or not protected. That's what we're going to investigate.

In terms of knowledge, yes, I maintain that most users of the Telus services probably did not know that their data would be used that way. We had a look at the privacy policies of Telus, and there is something in these privacy policies, as there often is in privacy policies of companies, informing Canadians that their mobility data, in a de-identified fashion, might be used for what they call “the public good”. They did not define “public good” to mean “used by the government and PHAC”. Be that as it may, we know these privacy policies are not read. They're long, they're complicated, and even lawyers have difficulty understanding them. That's not a particularly good way of informing Canadians of how their data will be used. I think in this case, the government probably did a better job through the COVIDTrends web page to inform Canadians. Be that as it may, I think it's fair to say that Canadians by and large were not aware and that more should be done.

Frankly, it will never be possible to inform people of all the uses that will be made of their information, because there are too many of these uses and many are legitimate or for the public good. If data is to be used for the public good, consent cannot be a precondition for all these public good uses. Consent has a place, and transparency has a place. Improving privacy policies has a place, but the real solution is to have a backstop to the absence of consent where you have objective criteria like legitimate commercial interests, which I agree probably need a bit of definition, or social good, enforced by somebody who can protect the interests of individual Canadians.

It's a complicated area. Let's not lose track of the fact that data can be used for good, but it needs to be better regulated.

The Chair: You have time for one last question, Mr. Bains.

Mr. Parm Bains: What's your standard for adequate protection of data?

The Chair: In 10 seconds or less.

Mr. Daniel Therrien: Is it for the social good, or for legitimate commercial interests, on one hand? On the other hand, does it violate privacy as a human right? Does it constitute surveillance? You balance these things out, and you determine whether the use of data is adequate in that fashion.

The Chair: Thank you very much.

With that, we conclude panel one of today's meeting. I'm sure all members will join me in thanking Commissioner Therrien and Mr. Turcotte.

I would like to proceed immediately to the second panel. I'm going to dispense with the procedural statements, because I think everybody was here, including our witness who was observing.

I'll suspend for a brief moment for a sound check, and then we'll begin panel two.

● (1200)

_____________________(Pause)_____________________

● (1205)

The Chair: We're resuming the meeting to begin the second panel.

Without further delay, I invite our witness, Dr. Khaled El Emam, to make his opening statement to a maximum of five minutes, following which we will have a single round of six minutes each.

Go ahead, Dr. El Emam.

Dr. Khaled El Emam (Canada Research Chair in Medical Artificial Intelligence, As an Individual): Thank you, Mr. Chair and members of the committee.

The purpose of my remarks is to offer an overview of de-identification. As someone who has worked in this area for close to 20 years in both academia and industry, perhaps this is where I can be helpful to the committee's study. I cannot comment on the specifics of the approach taken by Telus and PHAC because I do not have that information. My focus is on the state of the field and practice.

It's important to clarify terminology. Terms like anonymization, de-identification and aggregation are used interchangeably, but they don't mean the same thing. It's more precise to talk about the risk of re-identification. The objective when sharing datasets for a secondary purpose, as is the case here, is to ensure that the risk of re-identification is very small.

There are strong precedents on the definition of very small risk, which come from data releases by, for example, Health Canada, from guidance from the Ontario privacy commissioner, and from applications by European regulators and health departments in the U.S. Therefore, accepting a very small risk is typically not controversial as we rely on these precedents that have worked quite well in practice.

If we said that the standard is zero risk, then all data would be considered identifiable or considered personal information. This would have many negative consequences for health research, public health, drug development and the data economy in general in Canada. In practice, a very small risk threshold is set, and the objective is to transform data to meet that threshold.

There are many kinds of transformations to reduce the risk of re-identification. For example, dates can be generalized, geographical locations can be reduced in granularity, and noise can be added to data values. We can create synthetic data, which is fake data that retains the patterns and statistical properties of the real data but for which there is no one-to-one mapping back to the original data. Other approaches that involve cryptographic schemes can also be used to allow secure data analysis. All that is to say there's a tool box of privacy-enhancing technologies for the sharing of individual-level data responsibly, and each of those has some strengths and weaknesses.

Instead of sharing individual-level data, it's also possible to share summary statistics only. If done well, this has a very small risk of re-identification. Because the amount of information in summary statistics is significantly reduced, it does not always meet an organization's needs. If it does, it can be a good option, and that's how we tend to define “aggregate data”.

In practice, for datasets that are not released to the public, additional security, privacy and contractual controls must be in place. The risk is managed by a combination of data transformations and these controls. There are models to provide assurance that the combination of data transformations and controls has a very small risk of re-identification overall.

There are other best practices for responsible reuse and sharing of data, such as transparency and ethics oversight. Transparency means informing individuals about the purposes for which their data are used and can involve an opt-out. Ethics means having some form of independent review of the data-processing purposes to ensure that they are not harmful, surprising, discriminatory, or just creepy. Especially for sensitive data, another approach is a white-hat attack on the data: Someone is commissioned to launch a re-identification attack to test the re-identification risk empirically. This can complement the other methods and provide additional assurance.

All this means is that we have good technical and governance models to enable the responsible reuse of datasets, and there are multiple privacy-enhancing technologies, mentioned above, available to support data reuse.

Is everyone adopting these practices? No. One challenge is the lack of clear, pan-Canadian regulatory guidance or codes of practice for creating non-identifiable information that take into consideration the enormous benefits of using and sharing data and the risks of not doing so. This, and more clarity in law, would reduce uncertainty, provide clear direction for what reasonable, acceptable approaches are, and enable organizations to be assessed or audited to demonstrate compliance. While there are some efforts, for example by the Canadian Anonymization Network, it may be some time before they produce results.

● (1210)

The Chair: You have one minute, please.

Dr. Khaled El Emam: I've written a white paper with 10 recommendations for regulating non-identifiable data, which I can share with the committee if the committee wishes to review it.

To conclude, while I have not assessed the measures taken in this situation, I hope my comments can assist the committee's work.

Thank you. I welcome your questions.

The Chair: Thank you very much.

Before we begin, I'll remind all members that we are going to do a single six-minute round, so if anybody wishes to split their time, please indicate your intention.

With that, I'm going to begin with Mr. Brassard.

Mr. John Brassard: Thank you, Mr. Chair.

Dr. El Emam, I really appreciate your being here today.

Obviously, we're in the process of identifying some of the risks associated with the mobility data gathering of the Public Health Agency of Canada through a couple of organizations. I know you are an expert in this field of reidentifying de-identified and disaggregated data. Can you speak to the risks associated with that?

Dr. Khaled El Emam: If the data is de-identified using known practices, good practices, then the risks can be very small. There are many precedents from reputable organizations in Canada and internationally for what's deemed to be acceptable risk, and we can measure those risks and apply techniques to reduce the risk to be acceptably small. The methodologies have been well established and have been used in practice for some time.

Mr. John Brassard: Can you speak to some of those methods that can be used to reidentify such data?

Dr. Khaled El Emam: Yes, absolutely.

To de-identify information, there are transformations like reducing the granularity of the geography, to have larger and larger geographic areas, for example, or reducing the granularity of dates so you can have larger time intervals; instead of days, you can have weeks or longer. You can use synthetic data, which creates fake data that looks like the real data but it's not about the individuals. You can use cryptographic techniques, where you encrypt the data and do the analysis on the encrypted data.

There are a number of different technologies that have been developed that can be used for this purpose. The choice, of course, will depend on the objectives of the Public Health Agency and what kind of analysis they do, but there are options.

Mr. John Brassard: I've seen some studies and some reports. There was a European study done. The New York Times did an unbelievable study on how easy it is to reidentify data given one, two, three, four or five points of data being picked up.

Can you speak to those data points and the vulnerability with respect to reidentifying that data?

Dr. Khaled El Emam: If good methods have been applied, the risk of re-identification can be very small. I think that, in many of those examples, good methods were not applied. They demonstrate the importance of applying good methods and good practices.

As I mentioned, the risk is not going to be zero. There's always some risk. You manage that residual risk by putting in place additional controls, such as additional security controls, privacy controls and contractual controls.

Overall, the risk can be quite small. The approaches work well in practice when they have been applied properly.

● (1215)

Mr. John Brassard: The issue of consent is one that we've heard about as being important throughout this whole process. Oftentimes there's a convoluted requirement to provide consent, and oftentimes people aren't aware that their data is being tracked.

Can you speak to the importance of consent as well?

Dr. Khaled El Emam: As Commissioner Therrien mentioned, in cases like this it can be impractical to obtain consent a priori. Therefore, the de-identification methods and the additional controls and transparency and ethics reviews all provide assurance that the data is no longer identifiable and it's being used responsibly.

Mr. John Brassard: The other area you've been focused on.... I've read some of your work on synthetic data generation for privacy-preserving sharing of health data. The committee is not just looking at what happened with Public Health, but also looking forward and potentially making recommendations to the government on some changes that are needed in the collection of this data and ensuring that the privacy of individuals is maintained.

If you don't mind, could you just speak a bit more to synthetic data generation?

Dr. Khaled El Emam: Yes. The idea is that you start with the real data and you build a machine-learning or AI model that learns all the patterns in the real data, and then you generate new data from this model.

The generated data has no mapping to the original data. It has no mapping to real people. It's fake data that's generated from a model, but it maintains the properties and characteristics of the real data. You can do many kinds of analytics and surveillance—in this case, public health surveillance—using the synthetic data, but you have strong privacy protection at the same time.

Mr. John Brassard: Is the privacy risk diminished if you use this type of data generation?

Dr. Khaled El Emam: Yes. The risks will be quite small.

Mr. John Brassard: Thank you, Mr. Chair.

The Chair: With that, we will go to Ms. Saks for six minutes.

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

Thank you, Dr. El Emam, for joining us today. From the get-go, I'd like to say that I'm sure the committee and my colleagues here would be more than happy to see your white paper recommendations that you referenced during your opening remarks, to help guide us and help us be best informed as we move forward.

You mentioned in key points in data collection in this forum that transparency is essential. You mentioned that aggregated sets and how they're collected and presented are also essential, and that private contractors are a part of the social good, that they're using the appropriate guardrails in working through that data and providing it for use.

We've already established that the government was transparent throughout this process, starting in March 2020, with its indications for use of data. We've heard from the commissioner of a published framework available—to answer Mr. Green's request for it—of how to best use anonymized and aggregated data. Thank you for clarifying the difference; it's very helpful.

Regarding the importance of contractors we work with to collect this data being part of the social good, would you say that Telus and BlueDot—and we've seen BlueDot's report, which has been submitted to the committee—are generally among those practising for the good in their provision of data?

Dr. Khaled El Emam: I don't have the details of what BlueDot and Telus have been using their data for, but the current case of the Public Health Agency using mobility data to understand transmission patterns is a reasonable use of data for public health surveillance purposes.

Ms. Ya'ara Saks: You would say that, in this case with the pandemic and COVID-19, the use of aggregate data was for social good and a good purpose.

Dr. Khaled El Emam: Yes. As mentioned at the committee meeting last week, many countries around the world are using mobility data for public health surveillance purposes. It was also used before the pandemic by the UN, for example, to track movement of individuals, so it's not uncommon to do so.

● (1220)

Ms. Ya'ara Saks: Correct.

For clarification, the purpose of this study was to try to understand if the data that PHAC received, both through BlueDot and Telus, met the privacy criteria that you discussed in making sure that it was aggregated and anonymized when it was received by PHAC. In that case, in terms of the risks you were talking about and my colleague Mr. Brassard mentioned, would PHAC, from the data it received, be able to reidentify the data?

Dr. Khaled El Emam: I wouldn't be able to give you that answer because I haven't looked at the data and haven't done that analysis, but I think that's the objective of the OPC's investigation.

Ms. Ya'ara Saks: Following along those lines, we've already discussed that the data is important for health research, and you've indicated that you've been quite supportive of that. Have you seen, in any of the public discussions and in what Dr. Tam has shared in terms of COVID-19 Tracker, anything that would raise alarm bells for you after your many years of working in this field?

Dr. Khaled El Emam: The information that was presented in terms of public health surveillance is typical for the kind of information that would be used by other public health agencies for that purpose.

Ms. Ya'ara Saks: In this case, there have been a lot of numbers and information thrown around. I've heard 33 million. I think Telus would be thrilled to know they have 33 million customers. As far as I understood, the data collected from both Telus and BlueDot was more in the 14-million range, if that. Would that be a fair sampling of aggregate data that could be used on a nationwide scale by the Public Health Agency if it's aggregated and anonymized?

Dr. Khaled El Emam: If the objective was to do public health surveillance at a national level and if the data was distributed to have appropriate coverage, then yes, this would be a dataset useful for that purpose.

Ms. Ya'ara Saks: You mentioned surveillance, but I'd like to clarify that this is not surveillance of individual Canadians; this is an understanding of datasets of movement. Correct me if I'm wrong.

Dr. Khaled El Emam: Yes, it's public health surveillance to understand the transmission patterns of COVID in this particular case.

Ms. Ya'ara Saks: In this case, the Public Health Agency of Canada was not surveilling individual Canadians with the datasets that it received through BlueDot and Telus.

Dr. Khaled El Emam: Again, I can't comment on exactly what they did with that data, but the public maps and reports that are available are at the aggregate level, and they do not pertain to individuals.

Ms. Ya'ara Saks: Then have we met the initial criteria here of transparency in the aggregated sets in sharing that with Canadians through COVID-19 Tracker and other methods?

Dr. Khaled El Emam: For the reported numbers of that level of aggregation, it doesn't seem to pertain to individuals, but getting from identifiable data to that, I can't comment on the process, or who has handled it and what changes were applied along the way.

Ms. Ya'ara Saks: Okay. Privacy is obviously a big concern for those of us on the committee and also for Canadians in making sure that we do get this right and that what PHAC has done has been along the guidelines of the framework that was presented by the commissioner.

The Chair: You're just about out of time, Ms. Saks. I'm not sure we even have time to tack a question onto that. In fact, you're a little over.

With that, I'm afraid I'm going to have to go to Mr. Villemure.

[*Translation*]

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

Mr. El Emam, thank you for your insight.

Most importantly, thank you for not responding by confirming the findings conveyed to you as a question.

Have you ever worked for the Public Health Agency of Canada or the Government of Canada?

[*English*]

Dr. Khaled El Emam: I've been working with different departments of the government for almost two decades. I have worked with different parts of the government and Health Canada and the Public Health Agency during that period.

● (1225)

[*Translation*]

Mr. René Villemure: Of course. That is to be expected.

You mentioned that you were on a committee recently.

Were you recently invited to sit on a committee on behalf of the government or were you invited by other political parties?

[*English*]

Dr. Khaled El Emam: Which committee are you referring to?

[*Translation*]

Mr. René Villemure: You said earlier that you had talked about certain things recently at a committee meeting. I don't recall exactly what you said but I'm referring to what you said.

[*English*]

Dr. Khaled El Emam: I was referring to the committee presentations from last week with the Minister of Health.

[*Translation*]

Mr. René Villemure: All right. Thank you.

When you talk about disaggregated data or de-identified data, you are getting into some specialized jargon. What can the public understand here? We can all agree that we take privacy seriously and strive to maintain the public's trust as Canadians or as users.

So how can the public be expected to navigate a debate among experts about disaggregated or de-identified data? Customers using a cellphone to make calls or search the web don't know what that means.

[*English*]

Dr. Khaled El Emam: I think the key points are that we know how to do this quite well. The methods, the technologies, existed with this quite well. We need to make sure that organizations that are reusing data for legitimate purposes and for socially beneficial purposes are using and adopting these practices. Codes of practice and standards and guidelines that are precise and that can be enforced, or that are enforceable in some manner, would be one way to ensure that these good practices are adopted whenever data is reused for secondary purposes, and that will provide the assurance to the public.

[*Translation*]

Mr. René Villemure: Okay.

Do these standard practices you're talking about meet the minimum requirements, or do they provide ultimate protection?

[*English*]

Dr. Khaled El Emam: Ontario has de-identification standards. The Ontario privacy commissioner has published such standards, for example our guideline. These are good guidelines. They reflect good practices today. It's always necessary to update these on a regular basis, but I think having a national standard would be very helpful to ensure consistency across the country and for organizations that operate nationally.

[*Translation*]

Mr. René Villemure: If national standards were established, as the Privacy Commissioner of Canada is requesting, it would have the desired consequence of increasing public confidence in the secondary use of data.

[*English*]

Dr. Khaled El Emam: Yes, as long as you're also able to demonstrate that you have followed those standards, either through external audits or through some other mechanism.... Demonstrating it is important.

[*Translation*]

Mr. René Villemure: I agree, transparency and demonstration are important.

We've spoken a lot about the Public Health Agency of Canada. Now, let's talk about Telus. You are in the business, so you're familiar with the company. Can Telus be trusted to protect privacy in its commitments to put data to work for the common good? Or is that just a good front?

[*English*]

Dr. Khaled El Emam: I can only share with you what's known publicly. Telus's “data for good” program has won a privacy award this year from the International Association of Privacy Professionals, which is a highly respected association for privacy professionals globally. That's one indication that they have good practices in place.

[*Translation*]

Mr. René Villemure: So Telus is being recognized and it won an award this year.

Are there any risks involved in the Telus/BlueDot connection?

[*English*]

The Chair: Monsieur Villemure, I'm afraid you're out of time.

[*Translation*]

Mr. René Villemure: Okay.

[*English*]

The Chair: If the witness has a written response that he wants to provide later, he can, but we're going to have to move on to Mr. Green right now.

[*Translation*]

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

[*English*]

The Chair: Go ahead, Mr. Green. You have six minutes.

Mr. Matthew Green: Thank you, Mr. Chair. As always, I appreciate the opportunity for expanded written results and responses.

Through you to the subject matter expert whom we have here today, Dr. El Emam, I welcome him to the committee. I certainly want to acknowledge how much of this is new to me and, I'm sure, many of our colleagues in terms of the very highly technical nature of technology and where we are at right now with big data.

I'm going to rely on you to hopefully help us unpack this and explain it to me like I'm five years old. If you've already answered this question, I'd ask that you try to simplify it even more. In last week's presentations, I'm sure you'll recall that there was very specific language used around anonymized and de-identified data...and of course, from my perspective, the ability to hopefully get to some really solid recommendations from this committee to create gold standards internationally on having some of the highest rights-based approaches to data.

First, through the chair to the good doctor, given your role with Replica Analytics, do you work with countries internationally, around the world, on the emerging technology that you have created?

● (1230)

Dr. Khaled El Emam: Yes. I've been developing privacy-enhancing technologies for the better part of 20 years and deploying them through software and other mechanisms globally.

Mr. Matthew Green: In your opinion, which countries or regions—or which legislation, perhaps—could you point to that create some of the highest standards of a rights-based format?

I really appreciated the Privacy Commissioner talking about consumer rights-based laws and being able to provide those protections. Could you point this committee to some good examples that we might be able to include for consideration in our recommendations?

Dr. Khaled El Emam: In general, the GDPR in Europe is considered to be one of the strictest regulations for protecting individual privacy. I think the commissioner referred to that as well in his responses.

Mr. Matthew Green: For the purpose of this committee, can you explain exactly what that is and how you think the general data protection regulation could be applied to a Canadian context?

Dr. Khaled El Emam: That's a very good question. The regulation itself defines some general parameters, and the regulators have been developing opinions and guidance to operationalize the principles and the concepts around that. Also, there is the concept of codes of practice, which I think can be very helpful in terms of allowing the definition of standards and guidance that can be enforced as well. Of relevance to our current discussion, these would be two things to mention.

The GDPR has many other things that I think are beneficial, but we'd be here for a long time if we had to go through all of them.

Mr. Matthew Green: I appreciate that. I'm learning as I go along, as well. I see there are seven principles to the GDPR that talk about lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability.

I know in some of the past work that I have done around civil liberties, particularly as it relates to the way in which law enforcement uses information, we've heard stories of the private sector collecting data en masse for commercial use and then allowing that to be a back door for a surreptitious government collection of information.

Therefore, as it relates to things like storage limitation, or the purpose or use limitation, do you have any feedback that you would want to provide the committee based on the study we have before us today as it relates to mobility data?

Dr. Khaled El Emam: Purpose limitation, I think, is an important principle, and limits on data retention are also important.

There are different ways to operationalize that. One way to achieve the limited retention is to anonymize or de-identify the data after a certain period of time so it's no longer personal information. That intersects with our current discussion.

In terms of purpose limitation, we have to distinguish between personal information and non-personal information as well. Our conversation today is around non-personal information—

Mr. Matthew Green: I apologize for the interruption.

I ask this because I think one of the false definitions of the scope of this in the last two meetings was this idea that we ought to limit the conversation to just the way in which the federal government manages this information.

I would put this to you, Mr. El Emam, that at some point on the commercial side of this, prior to buying it from Telus, there would have been processes for the collection of this data. I would like to ask you, in your remarks, to reflect on the way in which the collection of data at the source could be held to the same standards that we would have internally within my own government.

I'll just share with you in a very clear way my concern, which is that perhaps we have outsourced privacy breaches to a commercial sector that might not have the same kind of rigour and, quite frankly, principles around purposeful limitation.

Could you comment on that quickly, or could you put it in writing for the benefit of this committee and for future recommendations we might have?

● (1235)

Dr. Khaled El Emam: Yes, absolutely. I'll quickly say a couple of things.

Companies need to collect personal information to conduct their business; that's normal. When they share that information with other entities, they would create non-identifiable datasets. Ensuring that this is done properly, plus the overlay of transparency and ethics reviews, provides a good governance model so that whoever gets the data has constraints or guardrails on what they can do with it.

That model is good when it's put in place. It works well in practice. We just need to make sure that it's put in place.

Mr. Matthew Green: Thank you, Mr. Chair.

The Chair: Thank you.

I think I let this slip and gave you a little extra there, Mr. Green.

At this point, I wish to thank our witness very much for attending today.

Voices: Hear, hear!

The Chair: We are going to switch to committee business.

Rather than going straight to in camera, I'll maybe open it up to members if they want to talk about our work plan. If we do want to discuss individual witnesses, maybe it would be best if we go in camera, if everyone is in agreement with that. That way we have the flexibility to discuss things that ought not to be public with respect to witnesses.

Go ahead, Mr. Brassard.

Mr. John Brassard: Thank you.

I would suggest that we go in camera to discuss it.

The Chair: All right.

Mr. John Brassard: I do want to say to Dr. El Emam that it's not often that a witness gets applause around here, but just so you know, sir, you did get applause from all of us. Thank you for your testimony today.

The Chair: Thank you.

With that, I will suspend as we transition to a different Zoom call for in camera.

[*Proceedings continue in camera*]

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

SPEAKER'S PERMISSION

Also available on the House of Commons website at the
following address: https://www.ourcommons.ca

Publié en conformité de l'autorité
du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

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