HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

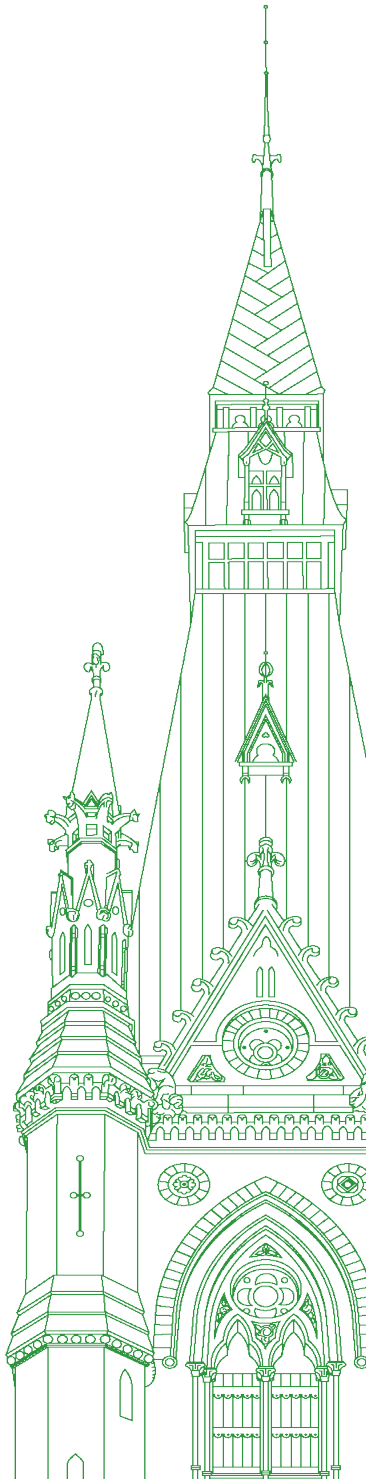
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 006

Thursday, February 10, 2022



Chair: Mr. Pat Kelly

Standing Committee on Access to Information, Privacy and Ethics

Thursday, February 10, 2022

● (1545)

[*English*]

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

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

We're starting late because of votes. I'm going to dispense with parts of the regular preamble. I think members are familiar with how we operate.

Pursuant to Standing Order 108(3)(h) and the motion adopted by the committee on Thursday, January 13, the committee commenced its study on the collection and use of mobility data by the Government of Canada.

Today, I would like to welcome our witnesses in this first panel. Our witnesses attend as individuals.

We have witnesses Ann Cavoukian, executive director, Global Privacy and Security by Design; and Teresa Scassa, Canada research chair in information law and policy, Faculty of Law, Common Law Section, University of Ottawa.

We will get right into the opening statements from our witnesses, which will be for five minutes each at the absolute maximum, please.

We'll begin with Dr. Cavoukian.

Dr. Ann Cavoukian (Executive Director, Global Privacy and Security by Design, As an Individual): Thank you very much, Chair.

I'm very pleased to be able to speak to you today because I was so concerned with the complete lack of transparency on the part of PHAC, the Public Health Agency of Canada.

Transparency is critical on the part of government agencies, of course. They report to individual citizens, and there was no transparency associated with PHAC accessing—I think they said it was 33 million—Canadians' cellphone data. I found it so disturbing.

I have to read one thing to you, which really resonated to me. MP René Villemure said that PHAC was using the data "without telling anybody". That, to me, is appalling. You don't just operate by yourself as a government agency, accessing people's very sensitive mobile data.

They didn't consult with the Privacy Commissioner of Canada, Commissioner Daniel Therrien. Commissioner Therrien said, "I do not think anyone would seriously argue that most users knew how their data would be used." Did the government inform users that their mobility data would be used for public health purposes?

The question of transparency and notice to individuals, to the public, of how information is being used on sensitive data such as mobility data is critical. On mobility data, when you track it, you know where people have been, who they've been associating with, their movements, etc.

I know you might say, "Well, but the data was de-identified—no problem." There are always problems. It's not a 100% solution, de-identifying data, as you know—phishing, hacking, ransomware.... This is huge. There are brilliant hackers who gain access to so much personal information, and the fact that no one was aware within the government that this was happening, and the total lack of transparency and notice, that's what concerned me enormously. I would say, privacy is all about control. It's about personal control relating to the use and disclosure of your personal information, and location mobile data, this is very sensitive. Nobody knew this was happening, and that's what I find so alarming, and that's why I'm focusing on the lack of transparency.

I want to suggest to you that it is high time for us to upgrade our privacy laws. PIPEDA, the federal private sector legislation, came in during the early 2000s. Our Privacy Act for the public sector came in during the 1980s. These are old statutes. We need to upgrade them and make them reflect what's taking place today in terms of the massive gaining of access to personal data and tracking the data and all kinds of implications and conclusions that could be made on the basis of that, without any notice being provided whatsoever. The public is not aware of the fact that this is taking place.

The fact that the government did this without consulting the Privacy Commissioner of Canada.... They'll say, "Oh, well, we told them." I know what the commissioner said. The commissioner said, "They informed us", but there was no consultation in terms of gaining input on whether this was appropriate or not.

Having served as a privacy commissioner for many years in Ontario, I'll say that it's absolutely critical to connect with the Privacy Commissioner and his team, where they can look “under the hood”, so to speak. I always say, “Trust, but verify.” These days, I don't even say “trust”. You need to look under the hood of the data-gathering practices and you need to make the public aware of what's taking place.

The Chair: You have one minute left.

Dr. Ann Cavoukian: This kind of openness and transparency is absolutely critical.

I'll end my remarks by emphasizing that these things can't be done quietly behind the scenes. No, the government has to be open and transparent, consult with people such as the Privacy Commissioner, and provide notice.

Thank you very much.

The Chair: Thank you.

For up to five minutes, Dr. Scassa, go ahead, please.

Dr. Teresa Scassa (Canada Research Chair in Information Law and Policy, Faculty of Law, Common Law Section, University of Ottawa, As an Individual): Thank you, Mr. Chair.

Thank you for the invitation to address this committee on this important issue.

The use of mobility data and the reaction to it highlights some of the particular challenges of our digital and data society. It confirms that people are genuinely concerned about how their data are used, and it also shows that they struggle to keep abreast of the volume of collection, the multiple actors engaged in collection and processing, and the ways in which their data are shared with and used by others. In this context, consent alone is insufficient to protect individuals.

The situation also makes clear that data are collected and curated for purposes that go well beyond maintaining consumer or customer relationships. Data are the fuel of analytics, profiling and AI. Some of these uses are desirable and socially beneficial while others are harmful or deeply exploitative. The challenge is to facilitate the positive uses and to stop the harmful and exploitative ones.

The situation also illustrates how easily data now flow from the private sector to the public sector in Canada. Our current legal framework governs public and private sector uses of personal data separately. Our laws need to be better adapted to address the flow of data across sectors. Governments have always collected data and used it to inform decision-making. Today, they have access to some of the same tools for big data analytics and AI that the private sector has, and they have access to vast quantities of data to feed those analytics. We want governments to make informed decisions based on the best available data, but we also want to prevent excessive intrusions upon privacy.

Both PIPEDA and the Privacy Act must be modernized so they can provide appropriate rules and principles to govern the use of data in a transformed and transforming digital environment. The work of this committee on the mobility data issue could inform this modernization process.

As you've already heard from other witnesses, PIPEDA and the Privacy Act currently apply only to data about identifiable individuals. This circumstance creates an uncomfortable grey zone for de-identified data. The Privacy Commissioner must have some capacity to oversee the use of de-identified data, at the very least to ensure that reidentification does not take place. For example, the Province of Ontario addressed this issue in 2019 amendments to its public sector data protection law, amendments that defined de-identified information for the purposes of use by government, required the development of data standards for de-identified data and provided specific penalties for the reidentification of de-identified personal data. The discussion paper on the modernization of the Privacy Act speaks about the need for a new framework to facilitate the use of de-identified personal information by government, but we await a bill to know what form that might take.

The former bill C-11, the bill to amend the Personal Information Protection and Electronic Documents Act, which died on the Order Paper last fall, specifically defined de-identified personal information. It also created exceptions to the requirements of knowledge and consent to enable organizations to de-identify personal information in their possession and to use or disclose it in some circumstances, also without knowledge and consent. It would have required de-identification measures proportional to the sensitivity of the information and would have prohibited the reidentification of de-identified personal information and imposed stiff penalties.

The former bill C-11 would also have allowed private sector organizations to share de-identified data, without knowledge or consent, with certain entities, particularly government actors, for socially beneficial purposes. This provision would have applied to the specific situation before this committee right now. It would have permitted this kind of data sharing and without the knowledge or consent of the individuals whose data were de-identified and shared. The same provision, or a revised version of it, will likely be in the next bill to reform PIPEDA introduced into Parliament. When that happens, some important questions need to be considered. What is the scope of this provision? How should socially beneficial purposes be defined? What degree of transparency should be required on the part of organizations that share our de-identified information? How will private sector organizations' sharing of information with the government for socially beneficial purposes dovetail with any new obligations for the public sector? Should there be any prior review or approval of plans to acquire and/or use the data, and what degree of transparency is required?

I hope the work of this committee on the mobility data issue will help to inform these important discussions.

Thank you.

● (1550)

The Chair: Thank you.

We go to the first questioner in the six-minute rounds.

Mr. Kurek, you have six minutes.

Mr. Damien Kurek (Battle River—Crowfoot, CPC): Thank you very much, Mr. Chair.

I appreciate both of the witnesses joining us here at the committee today and giving your opening statements. It's been very helpful that you've been able to share your expertise.

Dr. Cavoukian, you mentioned in your opening statement that privacy is about control. Certainly, we heard from the Privacy Commissioner about the lack of consultation and it appears to be the lack of control metric frameworks in place regarding the data that PHAC would have received. Can you speak more about the need for that control within a framework to ensure that data is protected?

● (1555)

Dr. Ann Cavoukian: I personally am a very strong believer in exercising control and allowing individuals to exercise control over the uses of their data. Traditionally, this has been linked with identifiable data. It has your name, address and other identifiers linked to it. Then, of course, you should be able to exercise total control.

There are means by which the data can be strongly de-identified, as has taken place here. Then our laws, the way they exist right now, no longer apply, because if data is considered to be de-identified, they no longer fall under privacy laws. That's one of the reasons I believe we need to upgrade our laws and reflect that in this day and age, even if you have strongly de-identified data—there are very strong ways of de-identifying data, and I'm not going to suggest otherwise—the risk of reidentification still exists.

I would like us also to explore other means of de-identification. For example, there are now new forms of de-identification that tend to have an extremely low risk of reidentification. This is called "synthetic" data, and this is now growing and being used.

What I'm urging is that people need to be able to retain control of their data, and especially with mobility data, which is so sensitive. I think if anyone had been asked...which PHAC did not do. If anyone had asked or given notice to the 33 million Canadians whose information and mobility data they gained access to whether they would have consented to that—no way, in my view. I think it would have been highly unlikely.

So I think we need to upgrade.

Mr. Damien Kurek: Thank you very much for that.

You started, I think, to answer the second question I had. It regards the ability to reidentify anonymized and aggregated data. Now, in terms of the government's response thus far, the minister a number of weeks ago said not to worry; it's anonymized and aggregated; just trust us.

Can you speak to some of the concerns that exist around reidentifying some of that data?

Dr. Ann Cavoukian: I want to be clear that they did go to great lengths to strongly de-identify the data and then use it in aggregate form. That does minimize the risk of reidentification. I don't want to suggest otherwise. I'm just saying that with mobility data—your cellphone, which lives with you and basically goes everywhere with you—there is such sensitivity associated with that and all the locations you go and who you may associate with, if the data were able to be reidentified and connections made on the part of the government, I think that would be extremely troubling.

So at the very least, the government should have provided notice to the public saying, "This is what we're doing. Here's why we're doing it. We want to track your movements in this COVID pandemic world." Is that a sufficient reason? Would people have felt the return was sufficient? We have to have some debate about these issues. PHAC can't just decide to do that, as the MP said, without telling anybody. That's what I objected to the most—the total lack of transparency.

Mr. Damien Kurek: I appreciate that. Thank you.

Part of the concern I have had is that I've seen a copy of a slide deck provided to the government by the company BlueDot. The information in that slide deck was very, very general and aggregated. But in the appendix, it spoke of very, very detailed information that BlueDot was receiving. Are you confident that the information that has been provided to public health...?

It seems to be more detailed than what that slide deck entailed, but we don't know exactly was meant by anonymized and aggregated. Are you confident that it has respected Canadians' privacy?

Dr. Ann Cavoukian: What you just told me I find very concerning, quite frankly. I understand the general data would appear very general and you couldn't get anything, but you just referred to data that was much more specific. That concerns me enormously.

That's why I want federal Privacy Commissioner Daniel Therrien to be looking under the hood at all of this. Why was he not consulted as opposed to just being informed? That's completely unacceptable. The minute you get into anything that is more potentially identifiable or detailed, as you were just describing, sir, that's when all the concerns arise. We can't have that.

● (1600)

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

I have one quick question for Dr. Scassa.

You mentioned that there must be standards for de-identified data. Are you confident that those standards exist within the information that's been provided for the government with the data that was used?

The Chair: You have 10 seconds, please.

Dr. Teresa Scassa: I don't have any direct knowledge of particular data standards that were used with respect to de-identifying the mobility data in question.

If legislation is going to extend to de-identified data, which it should, it should certainly extend to addressing or identifying what standards should apply, what de-identification standards should apply—

The Chair: [*Inaudible—Editor*] with further questions.

I'm going to have to go to Ms. Hepfner now for six minutes.

Ms. Lisa Hepfner (Hamilton Mountain, Lib.): Thanks very much, and thank you to the witnesses for joining us today on this very important issue.

I do want to come back to you, Ms. Scassa.

Last month you did a news interview. You spoke about how many of the stories around this mobility data issue focused on the government processing of the data rather than the fact that it's actually private companies that collect and sell location data.

Can you elaborate on why that's an important distinction?

Dr. Teresa Scassa: I think it's part of the overall data ecosystem, as some people refer to it, in which we find ourselves. It's that movement that I spoke about between private and public sectors, the flows of data from private sector to public sector.

There's a tremendous amount of mobility data being collected by all kinds of actors in the private sector. At the beginning of the pandemic and throughout the pandemic, companies like Google and Fitbit were publishing their analytics based on people's mobility data, analytics for Canadian cities and Canadian areas. This mobility data about us is collected by many different private sector actors and there are commercial applications for these data. As we can see in this example, government can be applying for that data.

I think that's why it's important that we need to think about modernizing both our private sector and our public sector data protection laws. We need to think about the way in which data flows from the private sector to the public sector and is then used by the public sector.

I think, in particular, that flow between public and private has been one that hasn't really been well considered in legislation in the past. Certainly the collection in the private sector context of these enormous quantities of data, and not just location data, but very fine-grained data about all of our activities, is a real issue.

Ms. Lisa Hepfner: Thank you very much.

I'd like to go back to you, Ann Cavoukian, to address a couple of things that you talked about in your opening statement.

First of all, there is no 33 million. That's a false number that keeps getting circulated. I just want to make that clear. Telus does not have 33 million customers. There's a lot of misinformation that's circulating—

Mr. Damien Kurek: Point of order. Tel—

The Chair: What is your point of order?

First state what is outside of usual practice or rule, and state your point of order.

Thank you.

Go ahead Ms. Hepfner.

Ms. Lisa Hepfner: Thank you. I appreciate that.

You were concerned about the lack of transparency. That was your point. Actually what we heard from the Privacy Commissioner when he came to speak to this committee was that he agreed the Prime Minister did put out a news release when the government started accessing mobility data from private collectors.

There is a public website where people at any time can check to see how this data is being used to inform the pandemic response. The chief public health officer, Dr. Theresa Tam, was regularly putting out messages on social media and in many other ways to show how this data is being used. I wasn't in government at the time but I knew this was happening.

The Privacy Commissioner, when I asked him, couldn't answer how the government could have been more transparent in this process. I'm wondering if maybe you can give us some suggestions about how the process could have been even more transparent than it already was.

● (1605)

Dr. Ann Cavoukian: With due respect, I don't call that transparency. I know Commissioner Therrien very well. He did not say his office was consulted on this, not at all. Being informed of something is very different from being consulted on something. You go to people to consult them, because they have expertise in an area.

As he said, he would have looked under the hood. It's essential to examine how information is being de-identified, aggregated and used for a variety of different purposes. Things can go wrong in a million different places. He may have also said, “I think we need to notify the public. I wasn't aware of any of this, as a member of the public, until I read the stories about it that broke out, all relating to the complaints associated with this, and the fact that John Brassard and others were saying nobody knows anything about this. It hasn't gone to the ethics committee. It was, in my view, not transparent.”

If you know what website to go to, and look underneath, you can find something. That's not transparency. In my view, you have to push it out, tell people, and tell the public what you're doing with their information and their mobility data. I'm not going to suggest there was transparency here.

Ms. Lisa Hepfner: Back to Ms. Scassa, can you talk about something else the Privacy Commissioner brought up, that it may not be realistic or reasonable to get meaningful consent in every instance, and yet mobility data is very useful in a public health response?

Can you comment on whether you see the usefulness of mobility data, and should governments have use of this data that has already been collected to respond to something like a pandemic?

Dr. Teresa Scassa: That question gets at something that is really at the heart of the digital and data society. There is such a huge volume of data being collected that it becomes impossible to rely on individual consent for all uses. Mechanisms have to be in place to supplement consent in some circumstances.

We don't have the time, the energy, nor the ability to manage consent for all of the data that is collected about us, and with everything that we do. Consent remains important, but it's not enough. Other measures need to be in place. There can be many socially beneficial—

The Chair: I'm sorry. Once again I'm going to have to do this. Our panellists will have to stop asking you questions, when they're actually out of time.

I'll move on to Monsieur Villemure.

[*Translation*]

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

Thank you, Ms. Cavoukian and Ms. Scassa.

Ms. Cavoukian, we are all well-informed people, but we had no idea what was going on.

Is a presumption of consent the same as meaningful consent? We have been told that people could not give their consent, so it was assumed that they did.

What do you think about this?

[*English*]

Dr. Ann Cavoukian: I don't think we can make any assumptions that there was a presumption of consent, not at all. I know consent is difficult. I agree that doing this on a large scale can be extremely difficult. I understand all of that. However, at the very least, provide notice, meaning you publicize. You are the government. You're PHAC. You publicize that you're doing this.

At the very least, you go to the Privacy Commissioner, you alert him, and ask for his input and assistance in making sure the public is aware of what's taking place. You alert him that it's being strongly de-identified and aggregated, and therefore the commissioner feels it's appropriate, something like that. You don't do it quietly, in my view. I think that's big mistake.

[*Translation*]

Mr. René Villemure: It's clear, then, that the presumption of consent does not equal consent. Similarly, publishing statistics on COVIDTrends is not the same as making the information public.

You spoke about trust earlier. In my opinion, the way they do things at PHAC triggers distrust more than anything else.

Would you say that the agency's way of doing things is unethical?

● (1610)

[*English*]

Dr. Ann Cavoukian: I totally agree with you. This grows distrust. There's already such fleeting trust anyway. Trust of government is diminishing on a daily basis, and this just leads to the further erosion of trust. I'm very concerned about that. Certainly, one would say you should be able to trust your government. I don't believe we're in a position to do that right now.

[*Translation*]

Mr. René Villemure: During his appearance, the minister said there was no need to worry, that all of the data were de-identified. Conversely, the Privacy Commissioner said that he was very concerned.

In your opinion, why was the commissioner merely informed, not consulted?

[*English*]

Dr. Ann Cavoukian: It's a very good question, sir. It baffles my mind. I honestly have no idea. When I served as commissioner in Ontario, I was always consulted. If I hadn't been consulted, especially on something like this, I would have been extremely concerned, because that's my business—to get under the hood and look at what's taking place.

I cannot imagine why the government—PHAC—did not consult properly with the Privacy Commissioner of Canada, Daniel Therrien, who is an excellent commissioner in this role. It makes no sense to me.

[*Translation*]

Mr. René Villemure: Situations like this one contribute to the erosion of public trust in government. In your opinion, this isn't a good thing.

On a scale of 1 to 10, how would you assess this operation by PHAC?

[*English*]

Dr. Ann Cavoukian: I hesitate to put a number on it, sir, only because I would probably give it the lowest number and I don't want to be unfair. I haven't examined everything.

This contributes to the erosion of trust enormously. There is already so much distrust out there. Let's leave it at that.

[*Translation*]

Mr. René Villemure: Okay. I completely understand your answer. I will assume that, for the moment, it is below 5.

People can't understand what is happening. Even if the government published statistics and press releases, it underestimated the need for people to understand what was going on. The government constantly threw up obstacles to transparency. It made the situation opaque. Like you, I learned about what was happening from the news. The ethicist in me was very worked up. I can't believe the government is continuing to deny the evidence.

Have you seen situations like this before?

[*English*]

Dr. Ann Cavoukian: I must admit that this was staggering to me. I had not seen anything on this scale with such a large number of individuals' mobility data being accessed without any notice to the individuals. Forget about consent, but just notice.... It's about public awareness, so that someone would know what was taking place.

When you take this to the Privacy Commissioner.... Had they consulted, the commissioner would also examine the benefit of engaging in this kind of access to the data versus what the results would be. They track people's movements. What is the benefit of that? I don't know. I say that as a question. None of this is open.

[*Translation*]

Mr. René Villemure: Dr. Tam also agreed that it wasn't very useful.

Do you think that this would have been possible if the European Commission's General Data Protection Regulation had been in force?

[*English*]

Dr. Ann Cavoukian: They have such strong privacy laws. The GDPR—the general data protection regulation—came into place in 2018. It is one of the strongest laws that exist. I was delighted that it includes my "privacy by design", which strengthens it even more, builds privacy and embeds it into the code of your operations. I don't think they could have done this.

Mr. René Villemure: I totally agree with you. I worked on the GDPR with the European Commission.

[*Translation*]

I am very surprised by what can happen.

Given the current state of affairs, what do we do?

[*English*]

The Chair: I'm sorry, but we're out of time on this one. We'll have to go to Mr. Green.

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

Welcome to all the guests. A really important discussion is being had.

Dr. Scassa, I thought your intervention provided some very direct points, which will hopefully be picked up in our study as recommendations. I want the opportunity to expand on that.

One of the issues I've had is the one that you've raised, which is the relationship between public and private data collection. I suggested in a previous meeting that it might be the case that our government institutions are basically outsourcing privacy breaches. I want to start from that frame through you, Mr. Chair, to Dr. Scassa, who identified this relationship between public and private data, and suggested, perhaps, that too much emphasis was being put on the government's possession of it and not enough on the private collection of it.

Dr. Scassa, in your opinion, could this program have been guilty of potentially outsourcing a privacy breach, for lack of a better term?

● (1615)

Dr. Teresa Scassa: That's an interesting question. I'm going to give a different example of the Clearview AI situation. You had a private sector company that created a facial recognition database based on scraped data that was then used by the RCMP. The Privacy Commissioner has already said that you can't have a legitimate use by a government actor of data that was collected illegitimately. That relationship is always interesting and it's an important one.

One of the challenges is that, on the one hand, you want to facilitate the use of data for socially beneficial purposes. The private sector is collecting vast quantities of data. There are legitimate questions in some cases about the quality of the consent, the quality of the collection practices and the kinds of data that are collected. In this case, we're looking at mobility data, which are very sensitive, but there are lots of other very sensitive data as well.

It becomes really important to think about that massive amount of data that's being collected under all sorts of privacy policies, which we don't have the time or even the skills to read and understand completely, that may become a product that is then sold to government, as well as to other actors, for their analytics. Right there, if there are flaws in that collection and it is sold, you carry over those flaws and those issues into the subsequent uses of those data.

That relationship is tremendously important.

Mr. Matthew Green: Let me put the question in another way. If the government had acquired the information directly, would that have been a cause for concern, in your opinion?

If there wasn't a third party, but the government was actively tracking citizens in this way through the security establishment or through cellphone towers, like we've seen with police using StingRay, for instance, or other Pegasus-type of—well, I guess that's still third party.

Dr. Teresa Scassa: I see your question and it's an interesting one. If the government is engaging in that kind of surveillance and there are certain rules that the government has to follow, specifically with respect to their collection of that data, and here it's being sourced from the private sector, it does fall under a different set of rules now. It's de-identified and so on, and it doesn't have the same weight or impact that surveillance data would, or the same implementations necessarily as surveillance data would have, depending on how it's used in the context. However, it's also data that the government doesn't really have the capacity to collect in that fine-grain and detailed way.

Again, the privacy issues are very important, but the ability of governments to use the best available data to make important public policy decisions is also important. The trick is finding that appropriate balance between the two.

Mr. Matthew Green: I agree with the appropriateness and the idea of what is deemed to be legitimate, even for the commercial interest. I referenced Google streets. You've been talking about Fitbit and Google.

I had my insurance policy renewal come up, and they talked about me putting an app on my phone that would track the speed to be able to give me a reduction in my rates, so I'm really concerned about the pervasiveness of the commodification of personal data and the way that it's being used as a bit of a panoptic prison.

Could you comment, Dr. Scassa, on international gold standards? We've referenced the European model, but in your opinion, which country has the highest standard of privacy and consumer protection and the separation between commercial and public interest? If you were to recommend to this committee an intervention that we can do to be the gold standard, what would that intervention be?

● (1620)

The Chair: You have 20 seconds left.

Dr. Teresa Scassa: Mr. Chair, the gold standard that is usually the reference point would be the GDPR in Europe and the rules that have been put in place there, with the proviso that there's no way to copy what's in the GDPR and transplant it to the Canadian context. Every country has its own particular context. It's not a question of saying, “Well, that's the one that we need to have”, but the GDPR sets an excellent standard.

Mr. Matthew Green: Thank you.

The Chair: All right. With that, we're out of time.

We're going to the next round. The next two questioners will have five minutes each, beginning with Mr. Patzer.

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

Thank you to our witnesses for coming.

Ms. Cavoukian, I think it's fair to say that for a lot of people out there who are having their location data collected without their knowledge or consent there is a level of trust that has been damaged and, quite frankly, broken. How important is public trust when it comes to an issue like this?

Dr. Ann Cavoukian: I think public trust is essential, in terms of building it, because it is fleeting right now. That concerns me so much. In the past, when I used to go and speak to public groups, I would have to explain why privacy was important and why I thought they should care about it. I don't have to do that anymore. When I go out and speak to the public, they are so concerned about it.

The public opinion polls in the last two years—from Pew Internet research and others—have come in at the 90 percentile in terms of concern for privacy. Ninety per cent are concerned about their privacy. Ninety-two per cent are very concerned about loss of their information. This is huge. I have been in the business for well over 20 years. I've never seen such enormous concern—consistently in the 90 percentile—associated with loss of privacy. The trust...or the lack thereof that exists right now with government is staggering. As I said, I've been in this business for many years. I've never seen it escalate as it has now.

The growth of surveillance that follows that is massive. A lot of times people say to me, “Oh, you just have to give up on privacy; it's just not possible anymore.” No, we don't give up on privacy. Privacy forms the foundation of our freedom. If you want to live in a free and open society, we have to have privacy, so I fight for this, even though trust is waning. Let's build it up. Let's get our governments to be honest with what they're doing with our information and at least notify us. Having it under the hood, not letting people know about it, just grows distrust, unfortunately.

Mr. Jeremy Patzer: I've seen some interesting commentary around the amount of surveillance that's gone on during the pandemic. When compared to what happened post-9/11, what's going on right now dwarfs what happened back then. I'm wondering if you have more comments on that.

Dr. Ann Cavoukian: I was commissioner during 9/11, and obviously it was enormously troublesome, but when 9/11 ended.... You see, during a crisis—a pandemic, an emergency—there are emergency measures that can be introduced to put the privacy laws on hold. The problem is that after the pandemic or emergency ends, often those emergency measures continue. Transparency goes out the door. Surveillance grows and continues to grow. That's what I'm concerned about with the pandemic now.

The pandemic, God willing, will be coming to an end. Measures are already being lifted in terms of our restrictions. We have to ensure that the measures taking place during these emergencies are suspended when the emergency is over, because we need to restore trust and we need to restore privacy. We can't have people believing that we just have to give up on privacy. No: You never ever give up on privacy. Privacy and freedom go hand in hand. They're both essential.

Mr. Jeremy Patzer: Thank you for that statement. That's very important.

I worked in the telecommunications industry for 10 years prior to being elected. It's my experience that people's data, whether.... Even as far as a smart home goes, your level of protection is only as good as the individual who's trying to access it.

Earlier, you mentioned synthetic data, but what else needs to be done, above and beyond the anonymized data, to actually try to really protect people? I've seen other reports. They had a sample of 100,000, and they were able to reidentify about 92% of all users, so there are obviously some issues. What more needs to be done here?

● (1625)

Dr. Ann Cavoukian: We have to get serious about getting the messaging out about privacy and the measures that need to be invoked at the time when the technology is introduced. A lot of people want to protect their home, so they have all kinds of measures to do that, but it often intrudes upon their neighbour's privacy, because the cameras capture information not just from that household but also from those around it.

Starting with what should be the appropriate restrictions on technology that is intended to be surveillance, what do you do about that and how do you minimize that in terms of its impact on others who don't want to be involved in it and who haven't introduced it into their lives and homes? These are the measures. We need to have measures that reduce the collection of data, of surveillance, and maximize the privacy choices that people can make.

The Chair: That's great. Thank you.

With that, I will go to Ms. Saks.

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

I would like to thank our witnesses who are joining us today. It's a very fruitful conversation.

Dr. Scassa, I would like to start with you, if I may. You made some important points with my colleague Mr. Green about the difference between surveillance data and mobility data. Telus for good was the sole-source contract in December 2020 through PHAC at that time. Prior to that, both the Prime Minister and Dr. Tam had been very clear that they were using the Telus data for good platform. From what I understand, that data was used by universities and others. University researchers, health authorities and others are using the Insights platform to collect really important data that we need during the health crisis. From what I understand they even received the seal of approval of the privacy by design certification on their work. That was the sole-service data provider to PHAC from the time of the public and transparent announcement that was made in April 2020 until the contract of December 2020 right through to October 2021.

In what you've described in this process, if you were a Telus user, would you be comfortable knowing that you could have opted in or opted out, knowing that data which PHAC used was not surveillance but mobility data?

Dr. Teresa Scassa: To be perfectly honest, I have no problem with my mobility data being used for legitimate public health purposes in the middle of a pandemic. I have more of a problem with it being used to push ads for cheaper coffee or whatever promotions as I travel around. For me that's more of a privacy concern than the use of my de-identified mobility data for socially beneficial purposes. I think this goes to the balance that we need to find.

Ms. Ya'ara Saks: Of course and I appreciate that. The Telus data for good platform was the sole-source provider to PHAC for that initial year. Dr. Cavoukian said to look under the hood. Well, the Privacy Commissioner was informed in April 2020 as well and didn't raise any alarm bells about looking under the hood at that time, and was informed, and from his own testimony had bi-weekly meetings with PHAC throughout the duration of that first year, and also in the preparation of the RFP for the forthcoming year after that.

Just so we're all clear on the process that has taken place, Canadians had ample access to public information whether they chose to.... Look, there's a lot of data and there's a lot of information in the news cycles as well. It's a really difficult thing to process what you are being told in the news cycle in the middle of a health pandemic, but Dr. Tam through COVID tracker and other sources was very transparent with the public of using data that was on a public platform.

Would you agree with that assessment, Dr. Scassa?

Dr. Teresa Scassa: I guess what I would say here is I think that part of the problem in this whole situation is the fact that we have companies and we have governments trying to do their best to address how to use data appropriately in this environment for socially beneficial purposes, but we don't have the updated legal frameworks that would apply to them. We don't have clear provisions that say, “This is what you need to do. This is the role of the Privacy Commissioner with respect to de-identified data. This is how transparency is achieved when data is shared for socially beneficial purposes and this is how we define those purposes.” All of this is taking place in this context where we don't have the modernized frameworks for this type of activity in place.

● (1630)

The Chair: There is just under a minute left.

Dr. Ann Cavoukian: May I add very quickly that Telus for good is excellent. I have no problem with that at all.

Ms. Ya'ara Saks: Thank you.

I think my time is up, Mr. Chair. Is that correct?

The Chair: You have half a minute. Go ahead, if you have another question.

Ms. Ya'ara Saks: Like all of us, I have one of these with agreements on them and so forth.

Dr. Scassa, through the chair to you, I really appreciated your comments on understanding that the client consumer relationship when it comes to these devices has dramatically changed in terms of the volumes of information that we're dealing with, and also of how they've become a part of our daily lives.

Perhaps you could provide a written answer to this. What recommendations would you want to see us consider going forward in tabling something like C-11, or recommendations for this committee to provide on upcoming legislation?

The Chair: It will have to be a written submission or later in the panel, because it is now time for Monsieur Villemure for two and a half minutes.

[*Translation*]

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

Dr. Cavoukian, I would like to ask you two questions and I don't have much time. The first question is simple, but you can answer the second one at greater length.

Some of the people that I spoke to during my career as an ethicist, and others that I spoke to about this issue, have said that, if you have nothing to hide, there shouldn't be a problem. I would like to hear what you think about that.

[*English*]

Dr. Ann Cavoukian: That always makes me laugh. That could have been the motto of the Stasi police and the Third Reich, because they would tell people, “If you have nothing to hide, what's wrong with the state knowing everything about you?” It is absurd. It's the exact opposite of freedom. Please, let us preserve our freedom. Privacy forms the foundation of our freedom. It's nonsense that you have to reveal everything to the world and to the government.

[*Translation*]

Mr. René Villemure: The relationship between privacy and freedom is clear, and we don't have to reveal everything to government or any other organization.

A call for tenders was issued for a second contract, and this committee made a unanimous decision to request the suspension of that call for tenders. A vote was held in the House on the matter yesterday. The request was made, and we don't know what will happen.

In the call for tenders, it was mentioned that the data could be used after the pandemic was over. Two things interest me. First of all, we don't know who will declare that the pandemic is over. Secondly, why would these data be used after the end of the pandemic?

[*English*]

Dr. Ann Cavoukian: That's what I would object to. As I mentioned, after 9/11 it was the same kind of thing.

[*Translation*]

Mr. René Villemure: Yes.

[*English*]

Dr. Ann Cavoukian: The measures that were introduced during 9/11 were intended to end after the emergency was over. They didn't. It's always a concern with measures that are introduced during something like a pandemic or an emergency situation, ensuring that they will no longer continue afterwards. I would be very concerned about that.

[*Translation*]

Mr. René Villemure: Okay. What would be your two main recommendations to improve the legislation?

[*English*]

Dr. Ann Cavoukian: I would want to be able to work with.... For example, the Telus for good program is excellent at de-identifying and protecting data. They have privacy by design certification. I'd want to work with them and with the government to see how we can make some uses of beneficial information while completely preserving our privacy or perhaps introducing synthetic data. Let's explore different options. This is what I would like to introduce in legislation.

[*Translation*]

Mr. René Villemure: Okay. I have only 10 seconds left, so I'll use them to thank you.

Ms. Scassa, unfortunately I didn't get the chance to ask you any questions, since my questions were directed mainly to Ms. Cavoukian. Thank you for joining us.

[*English*]

The Chair: Two and a half minutes goes by quickly.

Now we'll go to Mr. Green.

Mr. Matthew Green: Thank you.

Mr. Chair, I'd like to ask Dr. Scassa, who referenced an updated legal framework: What exceptions, if any, should exist with respect to the collection, use and disclosure of anonymized or de-identified information by the government?

Dr. Teresa Scassa: I was concerned by the wording in Bill C-11 in the exception for use of data for socially beneficial purposes that referred to the sharing of this data without knowledge or consent. I think that this transparency issue that Dr. Cavoukian has spoken about and that has been debated and discussed is fundamentally important here.

There need to be some transparency mechanisms so that people can understand how their data is being used. There may also need to be some sort of governance framework in place that sets parameters, puts limits on the use and sets an ethical framework for the use, if that's necessary.

● (1635)

Mr. Matthew Green: Thank you.

Mr. Chair, respecting the committee's time, I would just like to say to that point that the Privacy Commissioner has been clear as well with the recommendation that strengthening that office in a third party way would help them pursue that proactively as well as doing audits in the private sector, which I think would be an important point.

Mr. Chair, I'd like to now present this committee with a notice of motion that will be distributed by the clerk in both official languages. I'll use my last minute to do that so as not to take up anybody else's time.

Is that okay?

The Chair: Go ahead with a notice of motion.

Mr. Matthew Green:

> That, pursuant to Standing Order 108(3)(h) the committee send for, from the Public Health Agency of Canada (PHAC) and Health Canada, the Privacy Impact Assessment, and all documents used to inform the Privacy Impact Assessment, developed with regard to PHAC's use of mobility data tracking for COVID-19, and that these documents be received by the committee no later than March 4, 2022.

Mr. Chair, I'm happy to put that as a notice of motion. It's something that we should hopefully be able to debate and, with the support of this committee, pass and hopefully get that information to create a deeper understanding of what measures this agency took in pursuing this contract.

Thank you.

The Chair: Thank you.

With that, in the interest of making up some of the time we lost in this panel due to votes, I'm going to go to two minutes each for the last two questioners.

We'll have two minutes for Mr. Kurek and then two minutes for Mr. Fergus and that will conclude the first panel.

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

To Dr. Cavoukian, as Mr. Villemure mentioned, the concern in the RFP is that this data is not only going to be used in the fight against COVID, but it was very open-ended in terms of what the future use could be. I'm wondering if you have further comments on that.

I hope to get one more question in.

Dr. Ann Cavoukian: Having specific limits placed on use is absolutely critical. If you don't identify what the primary purpose or main use of the data collection is, secondary uses always arise. We can use it for this purpose or that purpose. A whole series of beneficial uses could be contemplated—

Mr. Damien Kurek: Sorry, I have a short amount of time.

I've heard from some constituents who are concerned that the data that the Public Health Agency of Canada may have received may not be limited to use within the Public Health Agency of Canada. It could be shared with other departments.

Is that a concern you would share?

Dr. Ann Cavoukian: Of course. How do we know what restrictions have been placed on the use of the data by PHAC or others in government? We know nothing. That's why looking under the hood by the federal Privacy Commissioner and auditing all of this is absolutely essential.

Mr. Damien Kurek: I appreciate that.

Certainly as a rural parliamentarian, I've heard also some concerns about the data that may be aggregated in an urban centre where there are hundreds of thousands or millions of people versus a small community where there are dozens or hundreds.

I'm wondering if you could unpack that in the little bit of time that is left.

Dr. Ann Cavoukian: The way in which these kinds of data are put together—as you mentioned, millions of people versus small communities—obviously if you have a very small community, it leads to the identifiability of those in that community. That's always a concern. That's why, again, you should always involve the federal Privacy Commissioner, who can examine all of that and make sure that the proper protections have been put into place.

The Chair: That's great timing.

Now for the final two-minute question round, we have Mr. Fergus.

Hon. Greg Fergus (Hull—Aylmer, Lib.): Thank you very much, Chair, and thank you to our witnesses.

I'm going to be very brief.

Dr. Cavoukian, thank you for your testimony.

I just want to make sure I understand. At our last meeting, Dr. El Emam talked about how there are really good ways to reduce the possibility of data being reidentified. He admitted that perhaps there's no perfect way, but there are world-standard practices to bring it down.

Does Telus data for good meet those requirements, in your opinion?

Dr. Ann Cavoukian: I would have to look at it hands-on. Telus data for good does amazing work. I have looked at Telus' work in other areas in terms of their de-identification of data and aggregation. They do an excellent job, so I agree with Dr. El Emam, who is the expert in this area, that they are doing it properly.

My concerns are not with the de-identification process followed by them.

● (1640)

Hon. Greg Fergus: Okay, so your concern is not about the de-identification process followed by—

Dr. Ann Cavoukian: It's about the transparency or lack thereof.

Hon. Greg Fergus: Sure.

I agree that there's a larger issue. Mr. Green's questions would speak to that or my colleagues would speak to that.

I'm really trying to understand what the Public Health Agency had received from Telus' data. Again, I think I'm hearing from you that you feel the information they received was de-identified to the best standard possible.

Dr. Ann Cavoukian: I'm sure it was. They are excellent in this field.

I want to repeat, my concerns were not with their methodology, it was with the government's lack of transparency in letting the public know what they were doing.

Hon. Greg Fergus: I just want to make sure, so Canadians can sort of feel, in terms of the information they got, that this wasn't government surveilling them. This was using de-identified data that came from a legitimate source.

Can I ask you just to confirm that?

Dr. Ann Cavoukian: Yes, I will confirm that.

Hon. Greg Fergus: Thank you very much.

On that front then, I want to also make sure that you feel—and if I could have you just clarify this—using that industry standard approach—

The Chair: I'm sorry, Mr. Fergus. I struggled to get my mike activated. You're quite out of time.

Hon. Greg Fergus: Thank you, Mr. Chair, for keeping me on the straight line.

I'm sorry I didn't have an opportunity with you, Dr. Scassa, as well.

Thank you to both of the witnesses.

The Chair: With that, I'm going to thank our witnesses.

Because of how badly over time we are, I'm going to suspend. Hopefully, we can very quickly sound-test our next panel's witnesses and begin the second panel as soon as possible.

The meeting is suspended.

● (1640)

_____(Pause)_____

● (1640)

The Chair: I call the meeting back to order. Now we'll begin our second panel of today's meeting.

I'd like to welcome our witnesses, Dr. Martin French, associate professor in the department of sociology and anthropology at Concordia University, and Dr. Daniel Weinstock, full professor in the department of philosophy at the Université de Montréal.

Dr. French, you have five minutes for your opening statement. That's the absolute maximum for opening statements, in the interests of time.

Go ahead, Dr. French.

Dr. Martin French (Associate Professor, Department of Sociology and Anthropology, Concordia University, As an Individual): Thank you, Mr. Chair and members of the committee, for the invitation to speak with you today.

I've been studying public health surveillance from a sociological perspective since 2003, when I started my doctoral studies. Over the years, since completing my doctoral work, I've continued to write about surveillance in public health and medical care contexts.

As a sociologist, I tend to prioritize different questions from the ones public health professionals might when considering public health surveillance systems. I share public health professionals' evaluative concerns that touch on questions of efficacy, efficiency, utility, timeliness and so on, but as important or even more important to me are social questions about how surveillance or its effects might be experienced by people in their everyday lives.

I'm interested, for example, in whether people might be advantaged or disadvantaged by surveillance. In my research, I tend to ask critical questions about public health surveillance systems. Perhaps it goes without saying, but I should also stress that while I ask critical questions, I am not against surveillance. In fact, I participate nearly every week in the FluWatchers surveillance initiative, which is operated by the Public Health Agency of Canada. This is one of the surveillance systems that provides data for the COVIDTrends website mentioned by Minister Duclos in his remarks before this committee.

I believe that public health surveillance can be valuable and I wouldn't want to see the Public Health Agency's innovations thrown out with the bathwater, but I'd like to use my time here today to put one critical question about equity on the table for the committee's consideration.

Members of this committee have been asking vital questions about privacy and consent in relation to the Public Health Agency's mobility tracking work. In addition to my fellow witnesses here today and witnesses from whom I believe the committee is going to be hearing in the days to come—Dr. Christopher Parsons, Dr. David Murakami Wood, Dr. David Lyon and others—these issues are going to be well covered. I want to say that I share the concerns of these witnesses.

I want to add an emphasis to what they're saying and a focus on equity questions, particularly this question: Who may experience intensified risks or harms as a result of mobility tracking?

In her remarks before this committee on February 3, Dr. Tam mentioned that mobility tracking could be used to understand the efficacy of public health measures. She stated:

> Mobility data at this kind of aggregated level can be used when provinces and territories or local jurisdictions enact public health measures to reduce contact rates or to ask people to stay at home, for example, to see whether those measures are actually working.

What would happen if these data were to show that people, for example, in a Montreal neighbourhood where I live, are not, in fact, staying home? Is it possible that these data would correlate to an intensification of policing or enforcement in that neighbourhood? I would like to know if the Public Health Agency of Canada is thinking about mobility tracking in relation to social scientific work on policing the pandemic, for example, led by Dr. Alexander McClelland, Alex Luscombe and the Canadian Civil Liberties Association.

Because of such equity questions, I would like to encourage the Public Health Agency and the Government of Canada to be more forthcoming in their discussion of emergent surveillance and contact tracing technologies. I think I'm nearly out of time, but I can give you an example of what I'm talking about with reference to the COVID Alert contact tracing application, if members want to pose questions about this.

Let me conclude by saying that I'm speaking today informed by the previous research that I've done and not from empirical data that I've been gathering about this particular mobility tracking initiative. I'll ask the committee members to please keep this limitation in mind while considering my preceding remarks.

I'll stop there. Thank you.

● (1645)

The Chair: Thank you.

We'll now go to Dr. Weinstock. You have up to five minutes for your opening statement.

Dr. Daniel Weinstock (Full Professor, Department of Philosophy, McGill University, As an Individual): Thank you.

I'm going to take 10 seconds of my time to correct the presentation that was made of me. I've been at McGill University for 10 years. I'm in the faculty of law and in the department of philosophy at McGill University.

I'm not an expert on privacy. My work has focused on a number of areas, but two that are significant or relevant to our present discussions are, on the one hand, the justification and the limits on the justification of rights limitations in a liberal democracy. What processes and arguments can be put forward in order to justify limiting standard liberal democratic rights and freedoms? I have done that across a wide range of rights, including religious rights. How do we justify the limitation of religious freedoms?

The other aspect of my work that is relevant to our discussions today has to do with the conditions of trust in government. What are the conditions? How does government make itself trustworthy, which is probably the most important question, and what are the mechanisms through which it can, in a legitimate manner, elicit the trust of the population?

There are relevant things to say in both those domains, and I'll say them quite briefly.

I live in Quebec, and my perspective is probably coloured by that fact. In general, there has been a kind of process in Quebec of what I would call armchair proportionality testing that has occurred in a fairly regular way, where the government has imposed upon itself to present to the population justifications of the fairly substantial restrictions that it has imposed on people's freedoms and rights, mobility rights, and rights of association. It has often experienced push-back, when it's been felt that either it hasn't shown there was enough evidence to prove that the restriction was one that was necessary to achieve the goal, or that perhaps it was overly restrictive, given the achievements of the goal.

There is a kind of parallel between the sort of formal demonstration of proportionality one finds, for example, in the Oakes test, and the kind of garden-variety proportionality testing that makes it the case that the population looks at restrictions that have been put in place, and says, “Okay, we may not agree totally, but at least there is an attempt at being transparent and public about these restrictions.”

● (1650)

[*Translation*]

Here's where I think data tracking is a problem: we are not dealing with restrictions. We are not dealing with measures that restrict the ability of Canadians to move around or to associate. Surveillance is relatively invisible, in that the objective is not to restrict our activity, but rather to measure it. The pressure on the government to justify surveillance is not as high as for a restriction. Obviously, when someone is told that they can no longer take part in a particular activity, they will demand a justification.

I think that the government may be tempted to not provide a justification, but it should resist that temptation. If it isn't open and transparent about the surveillance objectives and limits, whether they are limits in time or limits on the type of data being collected, the information risks coming out in a newspaper article and triggering distrust in Canadians. However, this distrust may be without cause. If the government had simply provided the same type of justification that it provides when it imposes restrictions, it is highly likely that the issue of trust and distrust would not have arisen.

In my opinion, that's the difficulty in this current context. There needs to be reflection not only about the measures that federal and provincial governments must take to justify their restrictions, but also about the measures that they must take to ensure that they don't trigger distrust among Canadians.

I will make a comment to the government that was made by a committee member when talking about the general public. If the government has nothing to hide about how it wants to use the data, why isn't it open and transparent? Why doesn't it get ahead of the issue by telling the media and Canadians its intentions and the specific and circumscribed methods that it will use to collect the data?

I'll stop there because I'm probably out of time.

[*English*]

I look forward to your questions.

The Chair: Thank you very much.

We'll go to our first round.

This will be six-minute questions beginning with Mr. Kurek.

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

First, thank you to our witnesses. I appreciate your coming to our committee today and sharing your expertise with us.

Dr. French, you talked about the FluWatchers app and the website, the platform and how that's informed some of the COVIDTrends data. A key difference there is that one is consent-based and one is informed by a whole range of other data.

Could you provide comment on the difference between consent for data being collected voluntarily or consent being directly given, versus some of the wide variety of collection that might have taken place on the COVIDTrends map?

● (1655)

Dr. Martin French: I can try.

On the FluWatchers, for example, I participate, as I mentioned, in that. I received an invitation to participate, I consented to participate, and I know that when I'm responding to emails the Public Health Agency of Canada is going to take that data, the information I'm giving them, and hopefully use it to inform their epidemiological work.

With mobility tracking, a number of members on this committee and witnesses have been raising consent issues, and I think that these are really challenging issues. In a lot of ways it's not clear to me, and maybe members of the committee could please correct me if I'm wrong about the specific details of this. Every member of the Telus network, for example, knew that if they didn't want to have their data included they should opt out.

I don't want to just impugn this particular initiative. I think this is a general cultural practice that we have of clicking “I agree”. I think Monsieur Villemure said this before in comments before this committee. It's just our culture today. We don't tend to read the terms of service and privacy policies, so we're not often aware. How could we be? They're often not written very clearly. They're not written to be read easily or understood.

This is, I think, a big problem. Many organizations say they're using personal health information, mobility data and other kinds of information. Even after they aggregate it, for example, de-identify it, there's still this kind of issue of consent maybe looming in the background more generally.

Mr. Damien Kurek: Thank you, Dr. French.

I don't mean to cut you off, but we do have a short period of time for questions.

I'm hoping to get this question to both doctors here.

You both reference the use of this data for its directed purpose by the government, but infer the possibility of there being unintended consequences, whether that be maybe different departments.... Even if it was aggregated or anonymized, the information may not simply stay within the Public Health Agency of Canada.

Dr. Weinstock, maybe I'll start with you. Would you in about 30 seconds, hopefully, talk about some of the concern that might be raised with that?

Dr. Daniel Weinstock: Yes, you've said it yourself. I think one thing that will increase trust in the process is if there are very clear, self-imposed limits by the government. This, of course, won't guarantee that there won't be leakage from one department to another, but it will give Canadians and watchdogs, like the privacy watchdog, a clear threshold, a clear benchmark on the basis of which they can say that what you've done here *outrepasse*—to use a French word—the limits you have imposed upon yourself in order to justify before Canadians the use of this data.

I think it's very important that there just be these very clear limits on the basis of which accountability can be very concretely based.

Mr. Damien Kurek: Thank you.

Dr. French, would you have a quick response to that?

Dr. Martin French: Just echoing that, I think that we know that early on in the pandemic first responders in Ontario, including police, were accessing COVID testing databases before the practice was stopped. We need to ensure that stronger firewalls are put in place around data that's collected for health and public health purposes.

Mr. Damien Kurek: Thank you very much.

I have a quick question for Dr. Weinstock.

There's the push-back on restrictions that I know this committee voted for unanimously, and then all the opposition parties voted to press pause on the RFP to continue this data collection. You talked about push-back on restrictions.

Do you have any comments on that and the need for the government to respect that push-back that's happened from both Parliament and committees?

● (1700)

Dr. Daniel Weinstock: If I understand the question correctly, I think we're in a very different time now than we were two years ago, which the government has to take into account. All I'm saying is, premised on the assumption that everything that's being done in this domain is perfectly justifiable. I think we are at a time where trust in government requires that that justification be done in a much more overt manner than might have been the case at the very beginning of the pandemic when the general population was, perhaps, willing to give a longer leash, as it were, to the government to act in the public interest.

The Chair: Thank you, Dr. Weinstock.

We'll go now to Mr. Fergus.

[*Translation*]

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

Mr. Weinstock and Mr. French, thank you very much for joining us today.

Mr. Weinstock, I am very interested in the last point that you raised. I listen to you quite regularly on Radio-Canada. You spoke about this just before Christmas, I believe. The trust of the general public depends on the context.

In the current case, the Canadian government did not conduct surveillance. It used de-identified, anonymized and aggregated data. As you just said, the public was more tolerant at the beginning of the pandemic.

Some of their de-identified data were used by provincial, municipal or federal governments to decide on the most effective measures in response to the pandemic. In your opinion, did that undermine the people's trust in government?

Dr. Daniel Weinstock: I will say two things very quickly.

I am not a data expert. When I was invited to appear before the committee, I did some due diligence. I asked some expert colleagues here, at the faculty of law, whether it's true that data can be completely anonymized. In both cases, they gave me skeptical smiles.

[*English*]

There's no such thing as completely “unpersonalizable”.

[*Translation*]

If there is a risk that what was initially used in a perfectly aggregated and anonymized fashion could then have personalized information reintroduced into it, then a precautionary approach must be used and measures must be taken to address the risk. The worst-case scenario needs to be used rather than the best-case scenario, if I can put it that way.

Once again, I am not at all hypothesizing that the current use of data by the government is wrong and reprehensible. I am simply wondering about the conditions that can inspire trust among the general public.

It's one thing to find out information from a National Post article that leads to Dr. Tam being called before the committee. It's quite another if the Prime Minister or Dr. Tam addresses Canadians ahead of time in an effort to be frank and open, expressing their view that significant public health objectives can be achieved by collecting these data, while ensuring that provisions limiting duration and use are put in place.

Hon. Greg Fergus: I'm sorry to interrupt you, but we have only six minutes. It's too bad, because it's a very interesting discussion.

Dr. Daniel Weinstock: You know, with two professors, it's difficult to—

Hon. Greg Fergus: —a philosophy student.

That's essentially what happened in April 2020. Dr. Tam said that aggregated, anonymized data would be used to measure certain things and that the information would be shared with all the health authorities across the country. The information was used, and there was a website on the topic.

That maybe didn't increase trust, but, at the very least, did it decrease the public's distrust of the use of these types of data?

● (1705)

Dr. Daniel Weinstock: In my opinion, it's important that an elected official be the one to do so. I may have misspoken when I said that it would have been the same thing whether the Prime Minister or the chief public health officer of Canada had done it. At the end of the day, decisions on issues as crucial and sensitive as data use should be entrusted to elected politicians. They are the ones who need to do this.

Across the country, there was a kind of confusion about what responsibility falls under public health and what falls under elected officials, particularly senior elected officials. I believe that it is the responsibility of political leaders, rather than of public health, to communicate with the general public.

Hon. Greg Fergus: How much time do I have left, Mr. Chair?

[*English*]

The Chair: You have a minute left.

Hon. Greg Fergus: Dr. French, again on this point, we had witnesses in the previous panel who are experts in privacy who indicated that the Telus data for good program, although not perfect, like Dr. Weinstock, when he was speaking to his colleagues...it certainly met the best practices possible to ensure that this anonymized information cannot be reidentified or cannot identify people afterwards.

From your perspective, is that sufficient or must we go for perfection? Is it sufficient to have industry leading standards or must we go further?

Dr. Martin French: I don't think we can reach perfection, but I think we should go further. From the research I've been doing, we do not—

Hon. Greg Fergus: We're talking about this from a Telus data for good program perspective. I want to make sure we're not speaking generally.

The Chair: Mr. Fergus, you actually used almost all of your time in asking your question. We're significantly over time now.

Hon. Greg Fergus: I'm sorry. I would ask the witnesses, if they wish to answer that, to send us some notes in writing. That would be helpful.

The Chair: Indeed, they can respond in writing.

Hon. Greg Fergus: We can incorporate that into the committee report.

Thank you.

The Chair: We're going to move to Monsieur Villemure for six minutes.

[*Translation*]

Mr. René Villemure: Good afternoon.

Thank you to the two witnesses, Mr. Weinstock and Mr. French.

To start, I would like to say that I do not believe that the intent of the Public Health Agency was malicious, as all of the witnesses have stated, by the way. I believe that the agency was probably well-intentioned. What bothers me is the way it went about it, which led to a lack of transparency.

Mr. Weinstock, the question that I would like to ask you is quite broad in scope.

In a polarized world, where people distrust rather easily... The current government has downplayed situations like those involving the Aga Khan and WE Charity. It's the same thing here. In fact, the Minister of Health trivialized the situation by saying that it was no big deal.

I am curious. What are the effects of this—almost commonplace— trivialization on trust in our institutions?

Dr. Daniel Weinstock: I will try to give a brief answer because I know that time is short.

Polarization is a multiplayer game. Responsibility for the current polarization is shared among a number of players. For example, the media are partly responsible.

A prudent politician, in the classic sense of the term, must be able to read the temperature of the room, in terms of polarization, in order to gauge how to communicate with the general public.

We are living in a time when the media are always on the hunt for missteps to increase polarization or draw attention. It may be a regrettable situation, but it is what it is.

I don't want to say that such and such a person is fully responsible for polarization, but it seems to me that elected officials should take action to reduce polarization. I'm not pointing fingers, but I feel that throwing oil on the fire simply creates scandals where none exist.

I agree with you that, in this particular case, it is highly likely that the data use is perfectly harmless. However, hiding things and overlooking the Privacy Commissioner makes it look as though something is something off, which has a tendency to fuel polarization rather than reduce it. That's unfortunate, in the current context.

● (1710)

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

In March 2020, the Prime Minister and Dr. Tam announced during a press conference that data would be used and that it could be tracked on the COVIDTrends website. It was on The Weather Network website.

Does that meet your definition of “making information public”?

Dr. Daniel Weinstock: I will be very honest. Two years of pandemic is a long time, and I think things that were said two years ago are worth repeating regularly. We have lived through so much, and there have been so many twists and turns in the limitations and reductions in terms of rights and freedoms that I don't think this matter can simply be removed from public debate once and for all, at the beginning of the pandemic, to never come back to it.

Mr. René Villemure: Okay.

Mr. French, I will ask you the same question.

In your opinion, do the COVIDTrends website and the press conference meet the sociological definition of “making a situation or information public”?

[*English*]

Dr. Martin French: I would like to see the Public Health Agency of Canada and the governments in Canada be more forthcoming. I feel they are doing a good job, but they could go further.

I mentioned the COVID Alert app, which is something I've studied. If we look at the privacy policy, which is on the website, objectively speaking, in terms of a landscape of privacy policies out there, it's pretty good. It's much more legible than many privacy policies.

Nevertheless, there are still...If you're an android OS user, you have to click through that policy to actually see the way the API works through Google Play to allow Google to access your location data.

I do think we need to go further.

[*Translation*]

Mr. René Villemure: Thank you very much.

Dr. Weinstock, I would like to hear from you about the course of events from March 2020 to present. The committee has met, we asked for the suspension of a call for tenders and the House has consented to it, but the government is not responding.

Do you think that this builds trust, or does it erode it and result in distrust?

Dr. Daniel Weinstock: That's difficult. That question could be considered leading.

Once again, these are partisan actions or reflexes that probably have no place in situations like this one. I believe that, at some point, Dr. Tam said that it wouldn't be the end of the world to wait a few weeks for the committee to submit its report. I think that the government is perhaps miscalculating the benefits and drawbacks of the partisan measures that it is taking. That means that Canadians may get the impression that there is something fishy going on, when that may not be the case. It's the height of irony to be in a situation where everyone is criticizing you for something that is baseless because—

[*English*]

The Chair: Thank you, Dr. Weinstock. You were over time, and I was just going to encourage you to wrap up.

I'm going to go to Mr. Green, for six minutes.

Mr. Matthew Green: Thank you.

It is certainly an incredible opportunity to have another panel of subject matter experts on this.

I want to pick up, and put the same question to this group of witnesses as I did in the previous group. I heard Dr. French talk about updated legal frameworks. What exception, if any, should exist with respect to the collection, use and disclosure of anonymized or de-identified information?

Dr. Martin French: Could I just ask for a clarification? Is it what exception in law should there be?

● (1715)

Mr. Matthew Green: I would say not just in law but in ethics, as in your research on privacy. We are always balancing the public good, and you had mentioned your support for the active use of what is being called “digital epidemiology” to provide evidence-based decision-making for our public health agencies.

What exceptions, if any, should exist with respect to the collection, use and disclosure of anonymized and de-identified information?

My hope is that coming out of this study, we'll have some prescriptive recommendations from this committee that will perhaps provide guardrails.

I'll give you another example. I presented in a notice of motion the idea of better understanding privacy impact assessments, and how the government processes the balance of those two considerations, when moving forward for the public interest.

Dr. Martin French: Thank you for that clarification.

I agree. I think that there's, let's say, a history in public health of crisis response. Understandably, public health has articulated surveillance systems to respond to crises, and sometimes these operate at a bit of a lower sort of oversight threshold because of the emergency nature of the response. I think that working with that culture, working to push that culture...let's say "enable the culture".... I think public health professionals have had a tremendously challenging time in this pandemic and being under-resourced, for example. Could we resource our public health professionals better to attend to things like these kinds of implications that I've been flagging, the privacy implications of the crisis decisions that they're having to make?

Mr. Matthew Green: Dr. Weinstock, before I get to you, I just want to carry on with that as a supplementary question.

Dr. French, you are quoted as saying, "There are populations that could experience an intensification of tracking that could [be] harmful...". This committee, in upcoming weeks and months, is going to be looking at AI, facial recognition and, as I referenced, the idea of digital epidemiology.

I was reading a review from the Canadian Public Health Association of Canada's initial response to COVID-19, which lays out all the ways in which our information is shared globally through the Global Public Health Intelligence Network. Could you identify any potential for concern, not just related to this, but also more broadly to ways in which AI could present a problem for some groups?

Dr. Martin French: This is a broad question. I'm not sure I can give a short answer to it, but I think there are historical examples of epidemiological data collected for good reason but being then subsequently used in stigmatizing ways.

I could point you to the 1982 publication of an article in the CDC's MMWR, the epidemiological weekly report, that identified Kaposi's sarcoma in Haitian communities, and we know that subsequently.... I could point you also to my colleague Dr. Viviane Namaste's work and 2019 book, *Savoirs créoles*, which talked about the experience of the Montreal Haitian community with this stigmatization that emerges post-1982. I'm thinking sociologically about these kinds of longer effects of specific programs, if I could put it like that in response to your question. I think we need to do better going forward.

Mr. Matthew Green: I'm going to say this, and this is not a stretch given where we're at in front of Parliament. We've heard today from Dr. Weinstock, who was talking about the feelings, and we know that through AI there could be the opportunity.... In fact, several Canadian universities are conducting research to develop analytical approaches on some of these challenges. They're using things like social media data in trying to sift through and find out where the public feeling is on particular issues to be able to shift some of our popular education and public education resources and our communications to, hopefully, offset this bit of a powder keg that we're seeing.

Would you care to comment on the use of digital epidemiology, for the lack of a better term, on that? Or, if you would, perhaps you could provide any additional comments in writing, as I know my time is now up.

Thank you, Mr. Chair.

● (1720)

The Chair: We'll have a 10-second response if possible.

Dr. Daniel Weinstock: It would probably be better if tried to provide you something in writing. I don't know how to say anything in 10 seconds.

The Chair: All right. Thank you. That sounds good.

We'll move on. We are going to end up going over time even with the second round.

My proposal is that I'm going to go with four minutes each for MPs Patzer and Bains, two minutes each for MPs Villemure and Green, and then just a one-minute question each from MPs Soroka and Khalid. That will take us to about five minutes over time.

If that's roughly acceptable, I'm going to proceed with that right now and go to Mr. Patzer for four minutes.

Mr. Jeremy Patzer: Thank you very much, Mr. Chair.

Mr. French, I serve a very large rural riding, and I think there's been a lot of concern from residents' being harassed by the government. They already live out in a rural area, are basically isolating by default and have been harassed about that.

When you look at the de-identified data, how much easier is it to reidentify data of people living in rural areas compared to somebody who lives in a massive urban centre?

Dr. Martin French: I don't think I have anything to add to this beyond what we heard from Dr. Cavoukian and Dr. Scassa today. I think it is the case that, the smaller the population, the greater the risk of identification in any kind of dataset, probably, but I'm not an expert on de-identification and reidentification.

Mr. Jeremy Patzer: In an article in the National Post, you mentioned some populations that could experience an intensification of tracking that could have harmful repercussions. I'm wondering if you could provide some context around that or a few comments there.

Dr. Martin French: Sure, I'll try. It was in a bigger email response that the statement was highlighted in. I was talking about what I think I've mentioned in my comments today, this possibility of other organizations using mobility data to guide their activities. It's not something that we know a lot about, but these data leakages, let's say, do happen from time to time.

I was simply trying to point to the fact that sometimes this mobility data can be used by organizations, like Dr. Tam said, to make recommendations or identify problems like people not obeying lockdown regulations or curfew.

My question is: What happens after that recommendation is made? Do we see an intensification of enforcement? If we do see intensification, does that potentially fall on communities that are dealing with other issues? Maybe they're doing shift work or what have you.

I'm not sure if I'm being clear in my answer, but—

Mr. Jeremy Patzer: That's helpful, so I appreciate that.

I only have about 30 seconds left, so I have a quick question for Mr. Weinstock.

I have a lot of constituents who are understandably angry and frustrated about basically having been spied on or surveilled and the data they're generating being used against them by the government. I'm wondering if there's a philosophical or an ethical argument there.

Dr. Daniel Weinstock: I think that there are important uses that could be made of data that, in other circumstances than that of a pandemic, we would expect to be private. Publicity on the ends to which this data is being placed, the limits on the use of the data, like temporal limits—when we are going to stop doing it, what the indicator is with respect to the pandemic that is going to make us say we're no longer in an emergency situation that justifies this extraordinary use of data—would go a long way in reducing some of that uncertainty.

● (1725)

The Chair: Thank you, Dr. Weinstock.

We will go to Mr. Bains for four minutes.

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

Thank you to both doctors for taking some time to join us today.

My question is directed to Dr. French.

You talked earlier about terms of reference, and we know that the de-identified mobility movements have an opt-out feature. In your mind, looking at government and these companies working together in the future, what can we do to look at those terms? You mentioned that the public doesn't really look at the terms of reference.

Dr. Martin French: Thank you for the question. I guess a brief answer would be a twofold answer.

There is a lot of work to do to educate people about data flows that are related to their use of mobile telephony. That is one thing. I would tend to like to see an opt-in approach rather than an opt-out approach, but I know that also has costs in terms of uptake, in terms of implementation. I think that's a debate but I would like to see an opt-in orientation.

Mr. Parm Bains: Right, but if we were to have an opt-in feature, doesn't that speak to the usefulness of the actual mobility movements? In this nature of the pandemic and working toward the public good, does the opt-in feature then just ultimately make this a not-so-useful exercise?

Dr. Martin French: I'm not sure how to answer that question. It is a great and a big question, but I'm not sure how to answer it.

I suppose we could hold the FluWatchers program, for example, which is an opt-in initiative side by side with mobility tracking, which is opt-out. I know that Dr. Tam said they give very different data.

I recognize that the Public Health Agency of Canada needs and sees a value in mobility data. I'm coming at this not as a public health professional but as a sociologist, so I also recognize that I have limitations in my kind of position. I want to make that clear.

I think that these are two different approaches to consent and from a privacy perspective, I would tend to favour an opt-in approach like FluWatchers.

Mr. Parm Bains: How much time do I have?

The Chair: You have about 40 seconds.

Mr. Parm Bains: I'll just say thank you for joining us, and I'll leave it at that.

The Chair: We thank you, Mr. Bains, for keeping us on time.

[*Translation*]

Mr. Villemure, you have two minutes.

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

Mr. Weinstock, I had a revelation earlier, thanks to you. I am assuming nothing, by the way. I am not assuming that there was bad faith or ill intention. My thinking was that it was difficult to strike a balance between protecting privacy and public health. You raised another point, though, and it made me wonder whether, at the end of the day, the difficult balance to strike was actually between partisan reflexes and public health.

I'd like to hear your opinion on that.

● (1730)

Dr. Daniel Weinstock: I believe that the first balancing act is still very important.

To pick up on the discussion between Mr. Bains and Mr. French, I think one of the things that makes the current situation really difficult is that the end goal of ensuring public health, which is assisted by data collection, can only be met if the vast majority of the population is enrolled in some way. That makes individual consent and the opt-in approach difficult. The balance is even more fragile when something like the opt-in approach serves the public good.

Concerning partisanship, we live in a political system where elections are held every four years. I think it would be nearly impossible to prevent politicians from looking at the election calendar and measuring their actions in part on that basis.

I would say that they sometimes miscalculate. In prolonged emergency situations—and I consider two years to be prolonged—people expect politicians to rise above partisan politics. Sometimes, actions that can be perceived as savvy political moves have a tendency to alienate the public's trust. I don't know whether what I said was clear.

Mr. René Villemure: It was quite clear. Thank you very much.

[*English*]

The Chair: We're now going to Mr. Green for two minutes.

Mr. Matthew Green: Mr. Chair, I'm going to try this again through you to Dr. French.

When I was talking a bit about the digital epidemiology and the use of data generated outside of our public health systems, I referenced social media. The reason I did that is because I'm looking for—in his opinion—where our limit should be. Right now, it's cellphone mobility data, but technologies are available with AI for the mass surveillance of public information. When that happens, I would argue that the use of social media raises ethical and legal considerations, including the de-identification of data and consent to its use.

Broadly speaking, just how far should the government go in the name of public health surveillance? In your opinion, where should it stop?

Dr. Martin French: This a debate that is happening in public health and beyond public health. In 2020, colleagues and I wrote a paper about contact tracing, talking about what we described as "corporate contact tracing" and raising questions for debates by public health authorities and scholars about an increasing reliance upon private sector organizations to execute their duties and responsibilities to the public at large. It raises a lot of difficult questions. In my mind, there's no clear way to draw the line.

The fragility of the public health system matched with the incredible data collection capacity of a number of private sector organizations makes it seem quite reasonable that we would turn to Facebook, etc., for data. Maybe that's a good idea, but there are also ways in which these public policy turns might drive more business toward these platforms.

The Chair: Thank you, Dr. French.

We're a little over time. I want to allow Mr. Soroka to get a minute in, and then Ms. Khalid will have the final word for a minute.

Go ahead, Mr. Soroka.

Mr. Gerald Soroka (Yellowhead, CPC): Thank you, Chair.

To Dr. Weinstock, you talked a lot about public trust of the government. The Privacy Commissioner offered to examine the data to determine whether it was declassified correctly, and the government declined.

Does that sound like building trust in the government?

Dr. Daniel Weinstock: That's a very good example. We have these mechanisms in place, which are the sorts of things that people can't look at under the hood of these very complex questions, but here's someone who has been nominated precisely because we think that's their job. When they're sidelined, it tends to raise suspicion that there is something to hide, whereas—and I insist on this point—there might not be anything to hide.

It becomes increasingly paradoxical that the government chooses to sideline a trust-building institution when, in fact, it could very well have been that had he looked under the hood at this data collection process, he would have found that everything was entirely ethically appropriate, from a privacy point of view.

● (1735)

The Chair: Thank you, Dr. Weinstock.

We have time now for Ms. Khalid, with the final word in one minute, please.

Ms. Iqra Khalid (Mississauga—Erin Mills, Lib.): Thank you very much, Mr. Chair.

I will try to be as brief as possible.

We've heard from witnesses that the use of data in informing health policy is quite useful, as it's balanced. We've also heard from witnesses that there is no perfect process by which we can maintain that transparency.

In your paper discussing the harm reduction approach and the ethical management of the COVID-19 pandemic, one of the principles that you apply this to is optimizing the use of space and time. Would you agree that mobility data would help increase the efficiency of protecting the public and making sure that there's a finer balance between restrictions and privacy?

Dr. Daniel Weinstock: Sure.

None of what I've said so far should be interpreted as me saying that I don't think we should be doing this. It's what tests we impose upon ourselves. I think that in Canada we have kind of proportionality thinking. Are we limiting people's freedoms too much? Are we showing that the limitation actually serves the end we're claiming it's serving? That's a good framework to do it in.

We also have agencies like the Privacy Commissioner that are tasked with doing that sort of thinking for us.

I think we might very well have ended up in a situation where he would have said that the use that's been made of this data is entirely proportionate to the very valid end that is being served. We just haven't had that demonstration from the kind of public body—

The Chair: I'm really so sorry that I must do this. We're getting excellent evidence for our study, but I simply can't allow it to—

Dr. Daniel Weinstock: I'm sorry.

We academics aren't very good at being concise.

The Chair: Don't apologize.

There is every opportunity, as well, for our witnesses to submit written evidence for the committee's consideration.

I'm sorry we had to go late, but I didn't want to shortchange both our panels, despite the vote.

With that, the meeting is adjourned.