HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

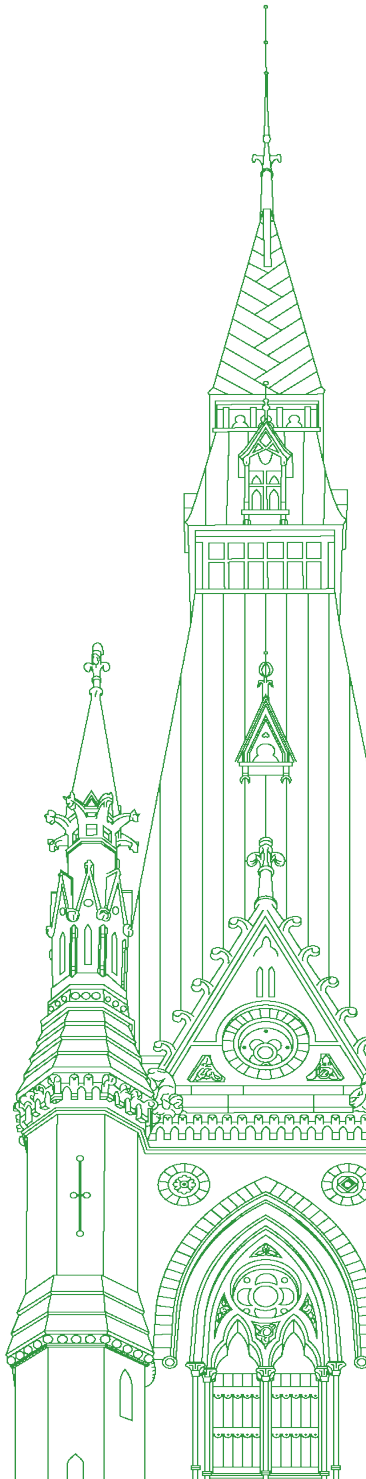
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 009

Monday, February 28, 2022



Chair: Mr. Pat Kelly

Standing Committee on Access to Information, Privacy and Ethics

Monday, February 28, 2022

● (1100)

[*English*]

The Chair (Mr. Pat Kelly (Calgary Rocky Ridge, CPC)): I call this meeting to order. Welcome to meeting number nine of the House of Commons Standing Committee on Access to Information, Privacy and Ethics.

[*Translation*]

Pursuant to Standing Order 108(3)(h) and the motion adopted by the committee on Thursday, January 13, 2022, the committee is resuming its study of the collection and use of mobility data by the Government of Canada.

[*English*]

Today's meeting is taking place in a hybrid format, pursuant to the House order of November 25, 2021. Members are attending in person in the room and remotely using the Zoom application. So you are aware, the webcast will always show the person speaking rather than the entirety of the committee.

I will remind members in the room about the public health guidelines. I understand that you have all heard them many times, so I'm not going to continue to repeat them, but I will remind participants that screenshots or photos of your screen are not permitted.

When speaking, speak slowly and clearly, and when you're not speaking, your microphone should be on mute. We'll also remind you that all comments by members and witnesses should be addressed through the chair.

I would now like to welcome our witnesses for the next hour. As individuals, we have Dr. Michael Geist, professor of law and Canada research chair in Internet and e-commerce law; and Mr. Jean-Pierre Charbonneau, a former Quebec parliamentarian and professional speaker on ethics. The witnesses will each have up to five minutes. I'm going to be strict on that so we can complete this panel on time.

We'll begin with Dr. Geist.

You have five minutes.

M. Michael Geist (Professor of Law, University of Ottawa and Canada Research Chair in Internet and e-Commerce Law, As an Individual): Thank you very much, Chair.

Good morning. My name is Michael Geist. I'm a law professor at the University of Ottawa, where I hold the Canada research chair in internet and e-commerce law, and I'm a member of the Centre for Law, Technology and Society. I appear in a personal capacity, representing only my own views.

I'd like to thank the committee for the invitation to appear on this issue, which represents an exceptionally thorny privacy challenge. I recognize that some of your witnesses have brought differing perspectives on the legality and ethics of this collection and use of mobile data.

From my perspective, I'd like to start by noting three things. First, ensuring that the data was aggregated and de-identified was a textbook approach to how many organizations have addressed their privacy obligations—namely, by de-identifying data and placing it outside the scope of personally identifiable information that falls within the law. Second, the potential use of the data in the midst of a global pandemic may well be beneficial. Third, it does not appear that there's a violation of the law, because the data itself was aggregated and de-identified. The public notice may not have been seen by many, but that, too, is not uncommon.

I think this creates a genuine privacy quandary. The activities were arguably legal, and the notice met the low legal standard. Telus, I think, is widely viewed as seeking to go beyond even the strict statutory requirements, and the project itself had the potential for public health benefits.

Now, there could have been improvements. The Privacy Commissioner of Canada, I think, should have been more actively engaged in the process, the public notification should have been more prominent, and there should have been opportunities—and should still be opportunities—for opting out, but I'm not entirely convinced that these steps would have changed very much.

The OPC would surely have pushed for more prominent notification and some assurances on the de-identification of the data, but it seems likely that the project would still have continued. Similarly, better notices would have benefited the few Canadians who paid attention, but I think we can recognize that it's a fiction to suggest that there are millions actively monitoring privacy policies or similar web pages for possible amendments. Yet, despite all of these factors, something doesn't sit right with many Canadians.

I believe the foundational problem that the incident highlights is that our laws are no longer fit for purpose and are in dire need of reform. It's not that I think we need laws that would ban or prohibit this activity. Again, most recognize the potential benefits. Rather, we need laws that provide greater assurances that our information is protected and will not be misused, that policies are transparent and that consent is informed. That doesn't come from baking in broad exceptions under the law that permit the activity because the law doesn't apply. Instead, it means updating our laws so that they contemplate these kinds of activities and provide a legal and regulatory road map for how to implement them in a privacy-protected manner. The need for reform applies to both the Privacy Act and PIPEDA.

With respect to the Privacy Act, there have been multiple studies and successive privacy commissioners who have sounded the alarm on legislation that is viewed as outdated and inadequate. Canadians rightly expect that the privacy rules that govern the collection, use and disclosure of their personal information by the federal government will meet the highest standards. For decades, we've failed to meet that standard.

The failure to engage in meaningful Privacy Act reform may be attributable in part to the lack of public awareness of the law and its importance. The Privacy Commissioner has played an important role in educating the public about PIPEDA and broader privacy concerns. The Privacy Act needs to include a similar mandate for public education and research.

With respect to PIPEDA, I would need far more than five minutes to identify all of the potential reforms. Simply put, the issue has inexplicably been placed on the back burner. Despite claims that it was a priority, the former Bill C-11 was introduced in November 2020 and there was seemingly no effort to even bring it to committee. The bill attracted some criticism, but this isn't rocket science. If Canada is looking for a modernized privacy law and wishes to meet international standards, the starting point is the European Union's GDPR.

Notwithstanding some of the recent scare tactics from groups such as the Canadian Marketing Association, the reality is that GDPR is widely recognized as the standard. Global multinationals are familiar with its obligations. There are innovative rules that seek to address the emerging digital challenges, and there are tough enforcement powers and penalties. There's room to tweak the rules for Canada, but we should not let the perfect be the enemy of the good.

● (1105)

Modernized privacy rules are not some theoretical exercise. As this recent event demonstrates, failing to implement those rules leaves Canada in a difficult position, with potential conflicting rules at the provincial level, compliance strategies that may still undermine public trust, and policy implementation choices that fail to maximize the benefits that can come from better data—

The Chair: Thank you, Dr. Geist.

[*Translation*]

Mr. Charbonneau, the floor is yours for five minutes.

Mr. Jean-Pierre Charbonneau (Former Quebec Parliamentarian and Professional Speaker on Ethics, As an Individual): Thank you, Mr. Chair.

First of all, let me introduce myself. I was the speaker of the National Assembly of Quebec for six and a half years and a parliamentarian for 25 years. I often lecture about ethics. I have written numerous texts and I have worked with institutes of ethics, particularly the one at the Université Laval. I am active in the Mouvement démocratie nouvelle, which is principally, but not exclusively, focussed on the reform of the voting system. I have been its president for some years.

To get tothe crux of the issue, we know that the Public Health Agency of Canada contracted Telus to collect personal cellphone data from millions of Canadians without their knowledge or consent.

There appeared to be no transparency in the operation, which theMinister of Health defended nevertheless. We also know that the Privacy Commissioner of Canada—we found this out very recently—had been informed about the government's intentions, but was kept at a distance from the process. The consequence is that basically three problems became clear.

First, in terms of ethics, the whole thing was done in secret. So the operation was hidden from view and Canadians were not told that the operation was happening.

Second, when the Privacy Commissioner of Canada showed up, he was basically kept at a distance. By keeping the Privacy Commissioner of Canada at a distance, the government made it impossible for one of the mechanisms in the act, namely the Office of the Privacy Commissioner of Canada, to play its role. Not only did the government keep at a distance the agency responsible for overseeing the way in which political leaders handle the protection of privacy, but it also acted in secrecy and made no apologies for doing so.

Third, the issue was normalized. When certain things were revealed and votes were held on the matter in the House of Commons, members who had passed the motion at committee ended up on the government side.

What is the consequence? When there is no transparency, when the behaviour does not use the mechanisms provided for in the act to protect Canadians and their privacy, their trust in the political institutions and in their political leaders, their elected representatives, is undermined.

Each year, there are surveys on the level of trust that Canadians have in their political leaders. Unfortunately, for years, all the political science studies tell us that the level of trust is very low. Each time something else happens, or there is another kerfuffle—a Toronto newspaper made this one public—that runs counter to the way in which leaders should behave, the public's trust does not go up, it goes down or it stagnates.

We need to recognize that trust is the basic building block of democracy. A democracy cannot work if the public does not have a minimum level of trust in their elected representatives, their political leaders.

These days, we can easily see how a dictatorship works. You don't need any involvement from Parliament. One man decides to send a part of the world into war, and there we are at war. Conversely, in a democracy, mechanisms exist. Mechanisms are a social contract between the public and its political leaders. The contract is built on trust, which is why democracies, like the parliaments in Ottawa, Quebec City and anywhere else, have provided themselves with mechanisms, codes of ethics and codes of conduct to safeguard that level of trust.

For example, the National Assembly of Quebec has a code of ethics and a code of conduct. One of the points in that code deals with the strength of one's word. I could have chosen others but that is one example.

Let me go back to this situation, this affair. As the previous witness said, it's not really the end of the world. It's not the scandal of the century in terms of affronts to privacy. But it is one factor in a number of factors that end up combining with a whole bunch of factors that, over the years, undermine the public's trust.

● (1110)

When we don't consider that to be important, when we normalize an event like this—

[*English*]

The Chair: I'm sorry. The time for your opening statement is just about up.

[*Translation*]

Mr. Jean-Pierre Charbonneau: Oh, my time is up all ready!

So I will wait for the questions, Mr. Chair, but I feel that I have said what had to be said.

[*English*]

The Chair: Thank you.

With that, we will proceed immediately to our questions.

We will begin with Mr. Kurek.

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

First, let me thank the witnesses for joining us and for sharing their expertise with the committee. I hope to get through a number of questions here, so bear with me.

We've heard from various privacy experts who have talked a lot about whether or not the data that was sent to the government met the necessary criteria for it to be truly aggregated and de-identified. The government's response largely has been to just trust them on that front. From both of your perspectives, starting with Dr. Geist, do you believe the government met the criteria to ensure that the data was in fact properly de-identified and aggregated and could not be reidentified?

● (1115)

Dr. Michael Geist: That's a great question. I think the starting point is the question of whether data can ever be reidentified. Can you put humpty dumpty back together again? I think that's one of the really exceptional challenges in this area. We see it play out on a lot of different issues.

From what I've seen in the testimony, certainly coming from the provider's perspective in terms of their responses and what they tried to do, it does sound like there was a genuine effort to try to ensure that it would not be identifiable, with various guardrails. I think it does come to the question that Mr. Charbonneau raised, the question of trust. If you don't have effective frameworks, if you don't have full transparency associated with this, if it's simply buried at the bottom of a web page that no one is going to take a look at, it's natural that people are going to raise these kinds of questions.

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

Mr. Charbonneau, go ahead.

[*Translation*]

Mr. Jean-Pierre Charbonneau: From the outset, the minister asked to be trusted. For political leaders to be trusted, they must behave in a trustworthy manner. When a government ignores the main body that Parliament has created to protect the privacy of Canadians, when the Privacy Commissioner is not involved and is kept at a distance, how can we completely trust this government or one of its ministers?

Once again, this is not the scandal of the century, but it is one of a number of scandals—some much more serious than others—that undermine people's trust. If the government is asking to be trusted, our answer must be that it must deserve that trust and that it must act legally and transparently.

Why was this operation done in secret? Why not clearly tell the public exactly what was going to be done, why it was going to be done and what the result was going to be?

One must not justify one's behaviour retroactively. One must be transparent from the outset, put one's cards on the table and use the protection mechanisms that guarantee—

[*English*]

Mr. Damien Kurek: I appreciate that. I think you both brought up some key questions.

To my next question, hopefully I can get a more or less yes-or-no answer from both of you. Did the government act transparently when it comes to the question that this committee is studying regarding the collection of mobility data?

Dr. Geist and then Mr. Charbonneau, please give as quick an answer as possible.

Dr. Michael Geist: I think—

[*Translation*]

Mr. Jean-Pierre Charbonneau: No. If it had acted transparently, we wouldn't be here today.

[*English*]

Mr. Damien Kurek: Thank you.

Dr. Geist, go ahead.

Dr. Michael Geist: I think it's hard to say that it has been fully transparent given the limited disclosure and the fact that the Privacy Commissioner wasn't more actively engaged. It's quite clear that this could have been done far better.

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

Specifically regarding the RFP, certainly what was troubling to me and many of my constituents as they reached out, as the media became aware and publicized the information around the issue we're discussing here, was the fact that this was not simply limited to COVID. The RFP talked about both COVID policy and the ongoing need for this data to be used by the government.

Do you think it's an appropriate path forward for the government to not only use data that was...? The government has defended the need for it during a public health emergency, but do you think it was appropriate for them to basically say that they need this data for the next five years for public policy without providing clear direction as to what that would be used for?

Dr. Geist, go ahead.

Dr. Michael Geist: I'd start by saying that keeping that door open is something that we see both companies and perhaps governments trying to do in terms of potential multi-use of data down the road. That's partially where these problems really start to arise. I think that you can make a credible case in some circumstances, but trying to leave full flexibility down the road starts to really tear at the public trust that we've just been hearing about.

If you have effective legal rules in place, then that simply isn't an option, because what you have to do when you have powerful legal rules in place is justify the use, and you try to circumscribe some of those uses so that they're more clear-cut and the consent itself is only valid for those narrow groups of uses, as opposed to essentially opening the door to alternative uses down the road as issues potentially arise.

Mr. Damien Kurek: Through you, Mr. Chair, I'll just confirm with Dr. Geist.

You do not see, then, that those frameworks are adequate to ensure that the information is protected.

● (1120)

Dr. Michael Geist: No, that was really the point that I wanted to drive home with my opening statement. I think that at the moment both the Privacy Act and PIPEDA simply are not fit for purpose.

The Chair: Thank you, Dr. Geist.

With that, we'll go to Mr. Fergus.

[*Translation*]

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

I would like to thank both witnesses here today.

I'd first like to turn to you, Professor Geist. I have been following your work on these issues for years. I have always appreciated your point of view.

Professor Geist, at the outset, you said—

[*English*]

The Chair: I'm going to interrupt you, Greg. I'm sorry. I've stopped your time. We are having some audio trouble in the room. The translation is just fine, but for those listening to just floor audio in the room, there was almost no volume.

Greg, this is your chance to squeak in an extra 10 seconds if you want to just give us a test on your volume.

[*Translation*]

Hon. Greg Fergus: I will keep going.

[*English*]

The Chair: That's much better. Time in and carry on.

[*Translation*]

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

Professor Geist, at the moment, we are specifically studying the Public Health Agency of Canada's use or possession of private cell phone data of Canadians, without their knowledge or consent.

In your testimony today, you said three things: that the data were de-identified to the extent that data can be de-identified, that the objective was beneficial because the data served to locate Canadians in order to check whether they were leaving their homes during the pandemic, and that it does not seem that we bypassed any legal standards.

That is the issue on which we are focusing our attention. However, you raised the issue, rightly, I feel, as to whether the current system is adequate.

Let me go back to the issue that we are concerned with. Can you state once more that the data were de-identified, that they could be beneficial in developing health policies, and that we did not overstep the standards?

Then, we are going to discuss the issue in depth.

[*English*]

Dr. Michael Geist: I must admit I'm not sure that I can answer that beyond having read the same transcripts that you will have seen, and therein lies part of the problem. Can I confirm for you that it was fully—

[*Translation*]

Hon. Greg Fergus: Perhaps not confirm, but—

[*English*]

Dr. Michael Geist: I can only go by what the committee has been told by Telus and responses from the minister. Based on what I've seen put forward, the indications are that that's the case.

I think it would have been better to have the Privacy Commissioner there operating as an independent agent to provide the kind of insight and review that may not have occurred in this case, and that's one of the shortcomings that we've seen.

It's easy to say that it's legal, but part of the problem is that it's legal. Part of the problem is that if we don't have strong enough consent measures and if we don't have a framework that imbues the kind of trust that we've been talking about, then you can both conclude that it's legal and still leave people uncomfortable with what's taking place.

[*Translation*]

Hon. Greg Fergus: I understand you completely, but the rules of the game require us to examine what is before us.

Some of your colleagues at the University of Ottawa, and some other experts, have said that the data were de-identified, as they were supposed to be, and the government received no information that could be used to identify people. So, not only the Public Health Agency, but also some experts in the area have come to that conclusion.

I assume that you share the opinion of those experts.

● (1125)

[*English*]

Dr. Michael Geist: I'm in line with the evidence that's been put forward to date.

I'm not an auditor. I'm not in the position, let's say, that the Privacy Commissioner would be in, to be able to go in and fully verify those statements. I'm able to go on the same publicly available evidence that they would be and that you would be, and based on that evidence, yes, it was de-identified. Telus made the case that they have a number of guardrails in terms of what was ultimately accessible to PHAC, so it's clear that there were steps taken to try to create those safeguards.

Again, if you're asking me to confirm based on some sort of inside knowledge, that isn't available. This program hasn't been transparent enough. I would ultimately trust the Privacy Commissioner's view, were they given the ability to go in and effectively audit what took place and then render a verdict on that question.

[*Translation*]

Hon. Greg Fergus: I'm going to ask you a question that you should like.

Let's set this specific situation aside and deal with the issue a little more broadly.

What kind of consent should Canadians be giving for their data to be de-identified and used for legitimate purposes?

[*English*]

Dr. Michael Geist: I think this represents one of the really exceptional challenges. We started to see that considered in the former Bill C-11, which included references to potential consent or potential rules even around de-identified data, and so—

The Chair: Thank you, Dr. Geist. Mr. Fergus was just out of time when he finished his question.

Thanks for the very brief answer. If you have more to add to that, maybe we can get that in later testimony, but it is now time for Monsieur Villemure.

[*Translation*]

Mr. Villemure, the floor is yours for six minutes.

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

Mr. Geist and Mr. Charbonneau, thank you for joining us this morning as witnesses. I will have one question for each of you.

Mr. Geist, we are looking at the situation from the point of view of ethics. A few minutes ago, you said that it seemed to be legal, and I will not argue that point. However, you will agree that something can be legal and unethical at the same time and that legality is the minimum required in order to operate, not the ideal.

Do you believe that the current rules are adequate?

[*English*]

Dr. Michael Geist: No, I don't think the current rules are sufficient.

I appreciate that the committee's mandate may be to focus on this specific incident and whether it was legal or not, but I fear that would miss the forest for the trees. There is an opportunity here to use this particular incident to highlight both the enormous value that the data can have, and then, by extension, the necessity of ensuring we have an effective data framework in Canada that includes adequate privacy safeguards, both within the federal government with the Privacy Act and in PIPEDA.

I think we can look at this incident as further evidence that at the moment we just don't have that.

[*Translation*]

Mr. René Villemure: Thank you very much.

Mr. Charbonneau, in the committee's work, we have learned that the Public Health Agency of Canada was dealing with Telus and that two other people were providing data to BlueDot, which was acting as an intermediary.

In a situation like that, do you believe the government could have done better to inspire confidence?

Mr. Jean-Pierre Charbonneau: The act provides a mechanism in the person of the Privacy Commissioner. There are almost 40 million of us and we cannot check everything. So we have a commissioner who, on our behalf, verifies that the processes are adequate. When the Privacy Commissioner is kept at a distance, the process is kept at a distance.

It's all very well to say that the actions were legal. I am not so sure about that, because being legal would have required the process to be followed and the institutions that provide protection and safeguards to be used.

Why is the government not using them? Because it makes things a little complicated and because the government may be afraid of the advice it might receive. It was probably afraid that the Privacy Commissioner might be getting in its way.

If you're not afraid, why not act transparently?

● (1130)

Mr. René Villemure: Thank you.

Mr. Jean-Pierre Charbonneau: Once again, you have to do that from the start, not retroactively.

Mr. René Villemure: Thank you very much, Mr. Charbonneau. I apologize for interrupting you, but we are limited in time.

Let me continue with Mr. Geist.

Which models could we use to better handle these situations?

[*English*]

Dr. Michael Geist: In the particular circumstance, I think there were a number of things that could have been done better in terms of the transparency of what took place. I think Christopher Parsons, who appeared before you, did a good job in his brief before the committee of identifying the lack of transparency and how this suddenly appeared on a website—

[*Translation*]

Mr. René Villemure: Excuse me a moment.

[*English*]

Dr. Michael Geist: —and the fog of information.

[*Translation*]

Mr. René Villemure: Let me interrupt you for a second.

If we leave the issue we are currently dealing with and we look at the situation as a whole, is there legislation that we could use as a model or that provides better rules?

Which models should we adopt?

[*English*]

Dr. Michael Geist: Yes, absolutely. Let me pick up on and extend some of the comments I made at the beginning with respect to PIPEDA on the private sector side, which would of course implicate the obligations that Telus and BlueDot would have faced. That's legislation that's more than two decades old at this point in time. We've seen multiple provinces now move ahead with their own legislation, given that the federal government has been so slow in moving forward.

We also have, as I mentioned off the top, the European GDPR, which is effectively the model that many are comfortable with and are already seeking to comply with. It seeks to address some of these kinds of issues in terms of algorithmic transparency, in terms of greater penalties, and in terms of identifying some of the newer sorts of issues such as the right to be forgotten, and others, which form a part of what I think is widely viewed as a modernized privacy law, something that Canada no longer has.

[*Translation*]

Mr. René Villemure: Finally, can you briefly tell us whether adding a privacy protection tribunal, as has been done in the case of the General Data Protection Regulation, the GDPR, is something that we should consider?

Mr. Jean-Pierre Charbonneau: Who was your question for, Mr. Villemure?

Mr. René Villemure: I am sorry. I was talking to Mr. Geist, who was still speaking at the time.

Mr. Jean-Pierre Charbonneau: Okay.

[*English*]

Dr. Michael Geist: Yes, on the issue of the tribunal, there was some opposition to that. A tribunal was proposed in Bill C-11. I actually had less of a problem with it. I thought that as long as it was an expert tribunal—which unfortunately Bill C-11 did not have; it had a mandate that one of the tribunal members have privacy experience, and I would think that if it's going to be authoritative, it needs to be a true expert tribunal in this area—there might well be value.

I recognize that the Privacy Commissioner has voiced some opposition to that, but I think that at a minimum we need to get a piece of legislation on the table. We can talk about what that administration looks like through committee study, but we're not even getting out of the gate on this issue.

[*Translation*]

Mr. René Villemure: Thank you very much.

[*English*]

The Chair: Thank you for that.

We will now go to Mr. Green for six minutes.

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

I definitely appreciate the idea of.... Going back to the forest, I would agree that this set of circumstances has opened us up for a much broader conversation.

My questions will be directed to Dr. Geist and are about some of the comments he made about the Privacy Act being outdated, being inadequate, and the need for the highest standards. I've been calling it the gold standard. In fact, the focus of my questioning has been along these lines for the entirety of the study, because I am looking to get out of this study recommendations that could strengthen our legislation so that we're not continuing to chase the ambulance, for lack of a better term, on individual instances of privacy breach but are creating a standard that meets or I would even suggest surpasses the GDPR. I say that because of the way in which information is being used politically—disinformation and all these other types of things—so it really does come down to being able to profile the end consumer of it.

So my question, through the chair, to Mr. Geist is this. Taking your time to walk through your top priorities to tweak the rules for Canada in a new and improved, modernized Personal Information Protection and Electronic Documents Act reform, what would that look like for you and how would that be the highest standard that Canada could put forward in this moment?

● (1135)

Dr. Michael Geist: I'll take a slight detour just to note that the Privacy Act, the part in terms of the obligations that the federal government has with respect to privacy, should not be overlooked at all. If anything, there's a core element there when we talk about the increasing desire for government, and some would say the need for government, to have more data in order to make better data-driven decisions, which may necessarily implicate data collection issues. In the case of the Privacy Act, that is even older in terms of when it was drafted and the failure to update it.

Mr. Matthew Green: Dr. Geist, this is a great opportunity. Maybe start there. What would be your top priorities for the Privacy Act?

Then could you use the remainder of your time to get into PIPEDA? I do believe you're quite right, that it is a process of holding both sides, government and private sector, accountable, because what we heard suggested...about what is legal versus what is ethical. Doing indirectly what you can't do directly remains a problem if we don't have a modernized reform on both sides.

Feel free to expand on that in whichever direction you'd like to take.

Dr. Michael Geist: Thank you for that opportunity.

I'll note that I've had the pleasure of appearing before this committee through multiple Parliaments. This committee has issued multiple studies on this question and made recommendations. There isn't a lot to rewrite here. It's one of these issues that just never seem to rise to the level of actual legislation.

Among the things we could do, I mentioned off the top the ability of the Privacy Commissioner to play a more proactive role in terms of public education and research about the relationship Canadians have with their governments in terms of the data that gets collected. We could also strengthen protections—for example, limitations on the data that government collects, so information is only collected where it is strictly necessary for its programs or activities. That hearkens back to one of the earlier questions of keeping the door open to other kinds of uses. There's a need to ensure that in fact it's the opposite: not only that we carefully circumscribe what gets collected, but that we identify that right from the very beginning.

In terms of breach disclosure-related issues, there is a need to ensure that if the data that is collected is put at risk—and we have had incidents in the past—the individual users themselves are adequately informed. Privacy impact assessments are necessary to ensure...and embed those within the law where some of these new programs are launched.

Then, when we think about this kind of issue in particular, which really opens the door to these large datasets, we need to think about the interaction that the federal government may have with private sector participants, because this represents a relatively new situation. It used to be the government might collect the data itself. Now we have, effectively, platforms or intermediaries that may be collecting some of that data and making it accessible to government. We need to establish effective precautions and safeguards in that regard. Was appropriate consent obtained? Is it de-identified? Have you worked with the Privacy Commissioner to ensure that's the case? Even if it was de-identified, what level of consent was obtained, as in this kind of case? Those are some of the things we could be, and I think should be, thinking about with respect to the Privacy Act.

In terms of PIPEDA reform, the way I would do it, to be totally candid, is to sit there with the GDPR text on the one hand, look at PIPEDA on the other, and then add in the bill that comes forward and engage in a benchmarking exercise to see where we stand. That's not to suggest that there can't be Canadian-specific reforms; I think there unquestionably can be. However, it is universally acknowledged that....

An easy one, of course, is the enforcement side of things. We don't have strong penalties. Our federal commissioner doesn't even have order-making power. That puts the federal commissioner in a position unlike almost any other privacy or data commissioner anywhere in the world in terms of not having the necessary tools to ensure effective compliance.

Then—

Mr. Matthew Green: I do apologize, because I have about 15 seconds left. As I tend to do, I invite both you and Mr. Charbonneau, who I know has lots of experience in this.... If there's a written submission on that particular question about those two features, the Privacy Act and PIPEDA, that you would like to make, I would love to see that referenced and be included in our recommendations and our study.

Thank you both.

The Chair: Thank you, Mr. Green.

Now we'll go on to Mr. Williams for five minutes.

● (1140)

Mr. Ryan Williams (Bay of Quinte, CPC): Thank you, Mr. Chair.

Thank you to our witnesses today. This has been great to listen to, and to see what the gold standard is, especially with GDPR and seeing what's happening across the globe.

One of the things I want to focus on today, to start, relates to GDPR. When we look at permanent versus temporary measures, has anything been written in that legislation or that protection in the EU to look at the difference between where we've had the measures through COVID and having to act on that side, which is a temporary basis, versus what would be permanent? Have you seen anything in there that would relate to that kind of thinking?

I'll start with Dr. Geist.

Dr. Michael Geist: Privacy laws are designed to be context-specific. They ought to be, and should be, adaptable to those kinds of situations.

In a situation where there are heightened concerns—let's say in a global pandemic or a war—some of the choices that get made and the balance that gets struck may well be different from those in other situations, which may be more mundane and don't raise those issues. The same, of course, is true depending on the sensitivity of the information. If we're dealing with sensitive health or financial information, the kinds of safeguards we'd expect may be different from questions about where I might have gone for lunch yesterday.

I think that the law itself is able to account for these different kinds of circumstances. The problem is that, if you don't have effective enforcement of those rules and you haven't modernized some of the consent-related provisions and the like, you're working with a very weak hand in terms of ensuring you have effective protections.

Mr. Ryan Williams: Thank you, Doctor.

Until we have more safeguards and, as you said, legislation in place that changes these rules, should Canadians have the option to opt out of data collection during, let's say, a pandemic or an emergency? I'm talking about something that's temporary instead of permanent. Or, in your thinking, would it make sense that we can't, that there are going to be safeguards in an emergency to keep that? When we look at a permanent versus a temporary situation in these laws, how are those rights of Canadians protected, in your opinion?

Dr. Michael Geist: I think it depends a little bit on the kind of data. It's an interesting question to pose: Can you opt out? Well, you can opt out, certainly, or you ought to have the right, I would say, to opt out of a program like this.

It doesn't seem to me that.... This is useful information, to be sure, and I think you can make a compelling case that it's valuable to have that sort of information, this kind of data. You see it play out in a number of different places. There's a lot of talk about waste water, for example, and trying to measure COVID-19 levels that way, as well.

We are anxious to get more data. The ability to opt out in those circumstances would seem to be appropriate. There might be circumstances, though, where the dependence of public health does require certain kinds of disclosures. We get that, of course, when we go into certain places and are required to disclose our vaccination status. That strikes me as entirely reasonable.

It seems to me that there are differences, depending on the circumstances in which this might be used and the data that's involved.

Mr. Ryan Williams: Thank you.

I do agree with you. I think when there's certain data, when we have to have personal data, there seems to be a different way.... We have to have safeguards with that. You mentioned waste water. It's not really easy to identify where that's from. There is facial recognition and certain other technologies, but what I'm focusing on is data that we're getting from individuals. I think that's where we are at.

Mr. Charbonneau, the committee has heard before from privacy commissioners that we should have done more to inform Canadians before the mass surveillance was undertaken. Would you advise the government to do that before it begins the next surveillance program, which is at tender stage right now?

[*Translation*]

Mr. Jean-Pierre Charbonneau: Let me emphasize once again that we have the Office of the Privacy Commissioner. Basically, the goal of that institution is to help political leaders and the public to see things clearly and, potentially, to find compromises or to assess risks for the public. It's impossible for everyone in Canada's population to provide an opinion. We have to have one entity representing the public and responsible for monitoring and protecting privacy—

● (1145)

[*English*]

The Chair: Thank you. We're out—

[*Translation*]

Mr. Jean-Pierre Charbonneau: …and determining how the government is behaving.

The Chair: I am sorry, Mr. Charbonneau.

[*English*]

I have to go to the next questioner. Mr. Williams didn't allow very much time for a response.

We will go now to Ms. Saks, for five minutes.

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

Thank you to our witnesses. Through you, Mr. Chair, I'd like to start with Dr. Geist.

I've read a fair bit of your work. Like my colleague, Mr. Fergus, I appreciate your insights. They are thought-provoking.

I want to talk about transparency, because that's something that's come up for you many times in terms of your own writings with regard to the government on a multitude of issues to do with the Internet.

On March 23, 2020, the Prime Minister's website announced publicly, and he did a press conference about it, engaging PHAC with BlueDot in order to collect that information and use it for the purpose of the pandemic. Then, only on March 26 did PHAC actually enter the contract with BlueDot. Then regularly after that, Dr. Tam, through COVIDTrends, Twitter and other platforms aside from the hard-to-read government website pages that we all get kind of bleary-eyed from at times, regularly updated what was happening through COVIDTrends and made announcements on an almost weekly basis. Then, in addition to that, there were the subsequent announcements about interacting with third party privacy assessors on the process. Then finally there was another public engagement on the correspondence with the OPC, the Office of the Privacy Commissioner, on a contract. Let's be clear: The contract was from 2020 until March 18, 2022, so throughout that time, we've heard about regular biweekly engagements with the Privacy Commissioner. A briefing was submitted, I believe, on February 14, 2022, wherein PHAC gave a final briefing and concluded that, according to section 3 of the Privacy Act, the data did not contain personal information.

So there was regular engagement on this. You've talked about what we could have done better with respect to the transparency. We're clear about the de-identified, anonymized part of it. In terms of that public conversation that you've alluded to, could you say how we could have done it better in terms of the spaces we're working in?

Dr. Michael Geist: Sure. I can try.

I would start by noting that my read of the commissioner's response was that he felt that his office should have been more actively engaged in this process, so I recognize it—

Ms. Ya'ara Saks: But I'm talking about the public transparency here, because that's what you alluded to.

Dr. Michael Geist: Fair enough. In terms of public transparency, I think your point highlights how this issue is often addressed by organizations, whether in the government or in the private sector, which is to say, “Hey, it was all there. All you had to do was go out and find it.” Most people don't know what BlueDot is. Even if they did, they still wouldn't necessarily know where the data was coming from or how it was collected down the line. So the need for full public education on this in terms of how that data would be collected in the first place, and then made more broadly available, is really important.

I was actively involved, for example, in the COVID Alert app discussions and was part of one of the studies that fed into that. There was a recognition that because you needed the public to actively install that, there needed to be a significant education program so that they would both trust it and understand it. You need to do the same kind of thing in this context where that kind of data is being collected—

Ms. Ya'ara Saks: So we're bleeding between consent and transparency here. I'm trying to understand where we could improve the government's transparency to the public on what we were doing. You're bleeding into the issue of consent on the actual interaction on the data.

That leads to my next question. We did have Telus for Good here, and Pamela Snively from their office went through a really detailed explanation of how their data platform is used not only by PHAC, in a very controlled setting with supervision, but also by universities like the one you are a part of and many other research institutions across the country, and how Dr. Ann Cavoukian in “Privacy by Design” actually extolled and praised Telus for Good in terms of the de-identified data that was used and the privacy standards they use.

In your opening comments, you stated that the pursuit of the perfect should not prevent the good. Now I can get back to what you were talking about. I really wanted to separate it out. What further steps do you feel the government could have taken to be transparent on the data?

● (1150)

The Chair: You have 15 seconds left.

Dr. Michael Geist: I'm just going to respond that in fairness, I don't think my response is shifting over to consent. I think my point with respect to COVID Alert and my point here is that if you want people to trust in these programs, you need to explain in as many forums as possible and as clearly as possible what data is collected and what's being used. That happened with COVID Alert. I'd argue that it did not happen in this context.

The Chair: Thank you.

With that, we'll go to Monsieur Villemure for two and a half minutes.

[*Translation*]

Mr. René Villemure: Good morning, Mr. Chair. I would like to introduce a motion that will be sent to all participants right away.

Let me explain the context. In our meeting on February 17, 2022, Mr. Khan, from BlueDot told us this:

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

The motion reads as follows:

> That the committee request BlueDot Inc. to file the names of its data providers by Monday, March 7, 2022, and that the analysts attach this information to the report of this study.

Versions are available in French and English.

[*English*]

The Chair: Thank you.

The motion is in order, because it is relevant to our present study.

We now have a motion before us. We have witnesses, and we like to make sure that we can have witness testimony. Are there any speakers to the motion, or may we put the motion to a vote?

It looks like Ms. Khalid wishes to speak to the motion.

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

I move to adjourn debate on this motion.

The Chair: Okay.

The motion to adjourn debate is not debatable. That will go straight to a vote.

Ms. Iqra Khalid: We can discuss the motion at subcommittee, if that's okay.

The Chair: Well, that's correct. We can discuss the motion in subcommittee, but a motion to adjourn debate has been moved.

We will go to a vote on adjourning debate on the motion.

Go ahead with the vote, Madam Clerk.

The Clerk of the Committee (Ms. Nancy Vohl): Thank you very much.

The vote is on the motion to adjourn debate on the motion by Mr. Villemure.

The vote result is five-five, Mr. Chair.

The Chair: I vote to adjourn debate. We will deal with this in subcommittee.

(Motion agreed to: yeas 6; nays 5)

The Chair: With that, we will continue with Monsieur Villemure.

You have the floor.

[*Translation*]

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

Mr. Geist, we are told that Telus' Mobility for Good program uses data for purposes that are socially beneficial.

Do you believe that this excuses Telus from obtaining—and I will be generous here—some basic form of consent from the users?

● (1155)

[*English*]

Dr. Michael Geist: The kind of consent required under the law does vary depending on the sensitivity of the information and the like. The fact that it's “for good” isn't really the factor that we would think about. We would think about the sensitivity of the data. We would think about whether or not the consent was informed and the like. The fact that this is for good purposes, in this case obviously in the context of public health and a pandemic, isn't one of the core questions we'd typically be thinking about in terms of the standard of consent.

[*Translation*]

Mr. René Villemure: Thank you very much.

In summary, adding the words “for good” does not really amount to a criterion for evaluating the appropriateness or the extent of any consent.

[*English*]

Dr. Michael Geist: No. I don't think it is.

[*Translation*]

Mr. René Villemure: Thank you very much.

Mr. Charbonneau, as you were interrupted earlier when you were making your comments, I'm going to let you continue what you were saying about trust.

Mr. Jean-Pierre Charbonneau: I was saying that trust is one of the pillars of a real democracy. A social contract connects the public with the political leaders, the elected representatives. That trust is fundamental. The more it's undermined, the more people feel entitled to do what they want.

The behaviour we have seen in recent weeks in Canada is the reflection of a problem of trust. If we want solidarity in society and we want people to observe the laws and the regulations, even though they may not like them, there has to be a very strong bond of trust between the people and their political leaders.

Without that trust, how do we plan to maintain people's allegiance to political institutions?

[*English*]

The Chair: Thank you.

We now have Mr. Green for two minutes, and then we will finish it out with Mr. Bezan and Ms. Hepfner.

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

Mr. Matthew Green: Thank you.

I have to name it. It's not lost on me that in a conversation around transparency, accountability and trust, a simple request for additional information was met with a procedural attempt to shut down additional information. I just want to say—

Ms. Iqra Khalid: I have a point of order, Mr. Chair.

Mr. Matthew Green: That's not a point of order.

The Chair: Ms. Khalid has raised a point of order. I'll ask her to immediately state which practice and procedure of committee is not being followed.

Ms. Iqra Khalid: I question the relevance of this argument. We're debating—

Mr. Matthew Green: That's debate.

The Chair: It's noted. I'll give the floor back to Mr. Green.

Mr. Matthew Green: I have limited time. The members of the governing side have ample opportunity to put forward the points of their debate. I invite them to do so in their own time.

I do have my two minutes. I will speak to the nature of this committee and my hope that when we're dealing with these issues, we can actually have open and public and transparent debates around the information that is provided both to the committee and to Canadians. That is part of the core of the problem in the functioning of this government, and one I'm going to continue to name. I'm just going to put on notice that as I see these procedural tricks, attempts to shut down information and attempts to filibuster, I will name it each and every time, notwithstanding the fact that I have my own motion that's going to be requesting more information. I put it on oral notice.

I ask members of this committee that we allow the fullness of the debate to happen in the public sphere, without this kind of instinct to constantly shut it down. It's a frustration I've had in my very short time here on the Hill, and one that I want to take this time to note.

Mr. Charbonneau, I did not get a chance to hear from you on those two questions. Given your learned experience in the National Assembly of Quebec, if you do have comments on things that were done particular to your experience in Quebec or in your time afterwards that you think would improve our Privacy Act or PIPEDA, I would ask that you please do submit them in writing. All of the evidence that is submitted at committee, as both you gentlemen would know, does become part of the study and hopefully will become part of the recommendations.

Thank you.

The Chair: With that, we will go to Mr. Bezan.

We are a little bit behind. I'm going to cut the last two down to four minutes each.

Go ahead, Mr. Bezan.

● (1200)

Mr. James Bezan (Selkirk—Interlake—Eastman, CPC): Thank you, Mr. Chair.

I'm excited to be part of the committee. I'm looking forward to working across all party lines and hopefully doing it transparently and out in the open.

I do want to give notice of a motion for the consideration of committee:

> That the committee immediately undertake a study of at least four meetings on the leak and misuse of personal data from crowd fundraising websites, and how the Canadian government can work to reduce these risks in the future; and that the first witness invited before the committee be the Privacy Commissioner of Canada.

I put that on notice.

I appreciate both Dr. Geist and Mr. Charbonneau for their comments today. I am very concerned about how data has been collected and how it could violate Canadians' privacy. The lack of transparency from the government and the concerns that have been raised by the Privacy Commissioner are troubling to all of us.

Dr. Geist, I read an article that you wrote in March 2020, at the very beginning of COVID. You also had a Globe and Mail op-ed. You mention standards and practices. You're talking today about the EU. You're also talking about how Israel and Taiwan are better at having those guardrails and transparency. Really, it comes down to the matter of trust, as Mr. Charbonneau was saying.

Do you believe there are enough guardrails in place, especially when you take a look at how long this data should be allowed to be held by organizations like BlueDot or by the Public Health Agency of Canada? I know you suggested in the past something like 14 days. Do we believe the government, through PHAC and BlueDot, is holding that information only for 14 days and then getting rid of it? Are they doing their analysis and moving on to help inform public information and public policy?

More importantly, how do we ensure that regulatory boundaries are in place that will, at the end of the day, protect the privacy of Canadians?

Dr. Michael Geist: Thanks for the question.

Thanks for bringing back some of the early stuff that was written at those very early stages of COVID. I think in some ways that really does highlight how essential it is to get the frameworks right to have the kind of transparency and the guardrails that we're talking about.

The last couple of years have been demonstrative of the need for both data and public active participation in different things. COVID Alert was a good example of that as well.

You can only get there if there is public trust in those collecting the data, in how it will be used and in the oversight that is in place. I think, respectfully, that we still fall short in that regard. The commissioner has raised these kinds of concerns. I don't think anyone is going to credibly try to question the commissioner when he raises these kinds of issues. That strikes me as a source of concern.

In terms of how long data is retained, that's a benchmark issue that exists within all modern privacy laws. One only retains data for as long as strictly necessary. If we're talking about specific trends data where we're trying to respond rapidly based on emerging trends, I would suggest that there is little reason to retain that data for lengthy periods of time once the value of it for that particular trend may have passed.

Mr. James Bezan: Mr. Charbonneau, go ahead.

[*Translation*]

Mr. Jean-Pierre Charbonneau: I am no expert in legislative drafting for the federal government, but I feel that the principle remains the same, that there should be a oversight mechanism. Earlier, we talked about improving the Privacy Act, but we already have an act and we are not complying with it. We also have an institution in place and it was ignored.

It is all very well to want to improve the act and strengthen the control and oversight mechanisms, but the challenge is to respect the institution that is already in place.

The Chair: Thank you, Mr. Charbonneau.

[*English*]

For the last four minutes, we have Ms. Hepfner.

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

Mr. Geist, I would like to go back to the line of questioning that my colleague, Ya'ara Saks, was examining. I don't think we heard a fulsome answer from you.

We were talking about transparency. You were saying that the government could have been more transparent with the rollout of this program. We heard that there was a news conference at the time when the program was started. There were regular communications from Theresa Tam on social media. As a journalist at the time, I was aware that the government was using mobility data to track whether pandemic measures were being followed and whether any outbreaks were likely to happen. I was aware that this information was being collected.

I would like to hear actual input from you on how the government could have been more transparent. Do we send a text message to everyone's cellphone? If there's a news conference, it's covered in the media. It's going out on social media every couple of weeks and there's a website you can refer to, so you can see how this information is being used.

How do we get more transparency into this process?

● (1205)

Dr. Michael Geist: I think that the—

[*Translation*]

Mr. Jean-Pierre Charbonneau: You could have more transparency…I don't know who that question was for.

[*English*]

Ms. Lisa Hepfner: Thank you—

[*Translation*]

Mr. Jean-Pierre Charbonneau: You could have more transparency by—

[*English*]

Ms. Lisa Hepfner: I was asking Mr. Geist.

Thank you.

[*Translation*]

Mr. Jean-Pierre Charbonneau: Ah, okay.

[*English*]

Dr. Michael Geist: Thanks for that.

I'll respond by saying that I do think.... I mean, you're highlighting a number of different things. I would say that COVID Alert does provide you with a better example of ad campaigns, of multiple ways of trying to advertise and communicate so that people are aware of what's taking place. To the extent to which we are accepting that there's some form of consent here, it is informed.

I think the COVIDTrends site could have made and still could make it clear where the mobility data is coming from, so that those Canadians who might be affected by it would know that's the case. I think the COVIDTrends website could include a link specifically to Telus's site, so that people who want to opt out of the Data for Good program would be in a position to do so. I think that they similarly could include a link to BlueDot to allow them to opt out of that.

If you have informed consent, it's about ensuring both: that people understand what is being asked of them or, more particularly, how their data is being used, and giving them the information they need to be able to opt out if they see fit. That, to me, is how you go about trying to ensure a high standard with respect to fostering public trust and complying with people's privacy expectations.

You can say, “Well, listen, we did this, this and this, and we were compliant with the law.” I thought I opened by indicating that this was, in my view, compliant with the law, but I think we'll come back to Mr. Charbonneau's point that compliance with the law doesn't always foster trust.

We want to ensure that we have trust, because this is important information, and these are the kinds of programs that can be critically important. Simply ensuring that we ticked the right boxes without necessarily going that extra mile to give people the kind of information they need to make informed choices and to be able to opt out, which are things that could be done.... To me, that would have been a better approach.

Ms. Lisa Hepfner: Just so we're clear, people did have....

Am I out of time? I'm sorry.

The Chair: Just ask a quick question. We have 30 seconds left.

Ms. Lisa Hepfner: How can we get better-informed consent from people using their cellphones and using these programs without jeopardizing the public health data that we need to...? Do you know what I'm saying?

How do we get proper informed consent so that people know what they're doing? You can opt out of these programs, but how do we get more awareness so that people can be more informed about it?

The Chair: Okay. With that, you've gone over your 30 seconds in asking your question.

Ms. Lisa Hepfner: Thank you.

The Chair: I'm going to invite our panellists, if they have further contributions that they would like to make to the study in answer to that question or any other, to do so in writing. They are welcome to do so.

With that, we are out of time for this panel.

I thank our two witnesses.

We are going to move into the subcommittee. Those members of this committee who are not members of the subcommittee can leave the Zoom call or the room. The subcommittee is in camera, so we will clear the room.

With that, this meeting is adjourned.