HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

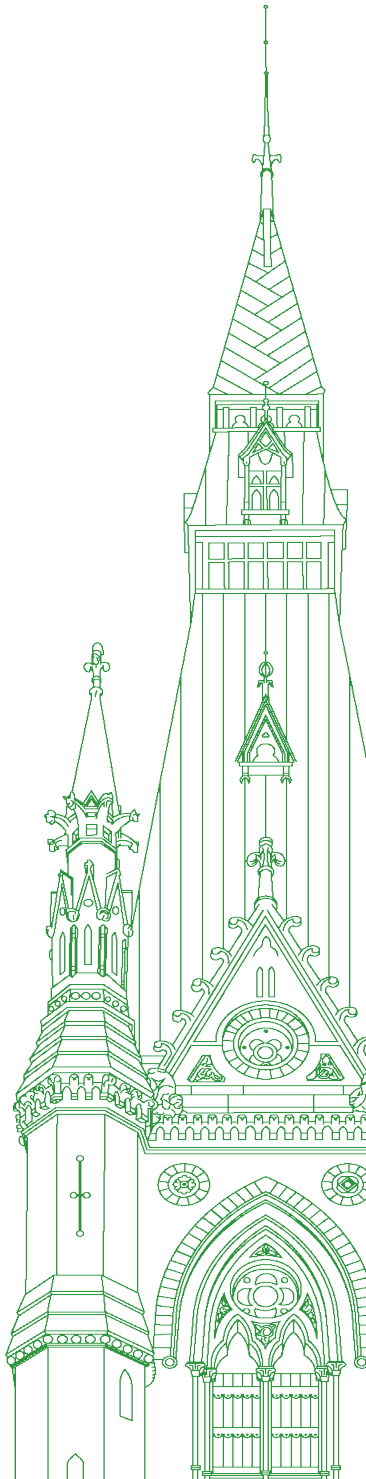
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 007

Monday, February 14, 2022



Chair: Mr. Pat Kelly

Standing Committee on Access to Information, Privacy and Ethics

Monday, February 14, 2022

● (1105)

[*English*]

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

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

Today's meeting is taking place in a hybrid format, pursuant to the House order of November 25, 2021. Members are attending in person in the room and remotely using the Zoom application. The proceedings will be made available via the House of Commons website. So that you are aware, the webcast will always show the person speaking rather than the entirety of the committee. I would like to remind everyone that taking screenshots or photos of your screen is not permitted.

With that, I'm going to dispense with the rest of it and get right to it. We have three panellists in the first panel. There is certainly the possibility of a bell interrupting this panel, which we'll deal with when we come to that. I mention it just so that everyone, including our witnesses, knows that we're going to quite likely have limited time. Even with three witnesses, it gets fairly tight.

With that, I would like to welcome our witnesses for the first hour. Appearing as individuals, we have David Lyon, professor emeritus of Queen's University; David Murakami Wood, director of the Surveillance Studies Centre and associate professor in the department of sociology at Queen's University; and Christopher Parsons, senior research associate at The Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto.

Welcome to our committee. I think we have remarks in writing from all three. It's up to you if you also wish to give your opening statement orally. There's an absolute maximum of five minutes to keep on time.

With that, we'll begin with Professor Lyon.

Mr. David Lyon (Professor Emeritus, Queen's University, As an Individual): I'm David Lyon, professor emeritus at Queen's University and former director of the Surveillance Studies Centre. I had a new book published recently, *Pandemic Surveillance*. That book acknowledges the importance and the risk of public health surveillance.

I am a historian and a sociologist, not a legal or technical expert. My interest in this case has primarily to do with surveillance using location data, which is the perceived issue in the arrangement for Telus to grant access to location data to the Public Health Agency of Canada.

A Globe and Mail article dismissed this as “a tizzy about 'surveillance'”, but whatever actually happened between Telus and the Public Health Agency, I want to say that surveillance is involved. Let me explain.

The concept of surveillance is being used in different ways. The alleged “tizzy” only occurred if what is happening is not really surveillance. The assumption here is that surveillance is defined in a way that highlights, say, police keeping a suspect under observation or intelligence agencies keeping watch on those suspected of terrorism. This would mean that specific people could be identified.

The committee was reassured by Dr. Theresa Tam that the location data was de-indentified, and by Minister Duclos that there was no surveillance here and thus no risk to Canadians.

I just want to make a point about the question of the definition of de-indentification. I'm not an expert on de-indentified data, but high-level studies from various places, one from Imperial College London and the university in Leuven, show that 99.8% of Americans could be reidentified in a dataset that used 15 demographic attributes. There is potential for reidentification, and therefore reassurances are required that the data are really secure and are used only for appropriate purposes.

Let me get back to the question of how we define this word “surveillance”. The Public Health Agency of Canada engages in surveillance. For the World Health Organization, surveillance is “the ongoing, systematic collection, analysis, and interpretation of health-related data essential to planning, implementation, and evaluation of public health practice.” The World Health Organization also notes the social and other dimensions of surveillance, warning that surveillance tools are not neutral and may be used in ways that challenge other priorities such as human rights and civil liberties.

This committee was informed by Dr. Tam that the location data was used for at least two purposes: to discover whether lockdown measures were really being observed and to discern the geographical spread of the virus. We must note that the meaning of "surveillance" has expanded considerably over the past few decades. The police or security definition often includes monitoring, tracking or profiling a suspect. This may mean trawling through datasets containing identifiable data. In North America, such surveillance is often qualified by the word "electronic"; in the European Union, however, the simple word "surveillance" is routinely used to cover many kinds of data collected [*Technical difficulty—Editor*] use, both in the public sphere and in the private, such as targeted advertising.

I would say that surveillance is really the focused, routine and systematic attention to personal details for specific purposes, such as management, protection or influence. It includes individual scrutiny such as monitoring of suspects, but also an interest in population groups. Surveillance is whatever makes people visible. Whether it is done with individualized, identifiable means or whether it has to do with population groups, either is risky, as the WHO points out. People are being treated differently, either as individuals or as groups.

● (1110)

Today, in a situation where we have almost ubiquitous use of smart phones generating huge quantities of data, including location data, their use depends on the analytic power of large organizations, public and private. Many prize that data. It was misused in China and Korea, for example—

The Chair: Thank you. I am going to have to move on. We're on a very tight schedule.

Thank you for your remarks, Professor Lyon.

Professor Wood, go ahead, please.

Dr. David Murakami Wood (Director, Surveillance Studies Centre and Associate Professor, Department of Sociology, Queen's University, As an Individual): Hello. My name is Dr. David Murakami Wood. I'm the current director of the Surveillance Studies Centre at Queen's University and associate professor in the department of sociology. I have a similar background to that of Professor Lyon, although, obviously, I'm less eminent and have had a less lengthy career at this point.

I thank Professor Lyon for his observations on the term "surveillance". I am going to skip over those areas, because I did have some observations in my submission.

What I want to do in my brief remarks is simply outline the potential problems with respect to surveillance in this case and the possible benefits.

I think the first thing we need to observe here is that it is not unusual for public agencies of any kind to obtain and use datasets. This, I would argue, is the basis of any evidence-based policy-making. In fact, the fact that surveillance is being conducted is not in itself a de facto form of human rights violation or anything else. This can be an extremely good thing.

I also want to emphasize that at no stage has there been any credible evidence, or even a suspicion, of individual tracking or surveillance at that level, of the kind mentioned by Professor Lyon. This was population-level, anonymized and aggregated data, and in some cases already analyzed. It's technically possible to disaggregate and de-anonymize data, but in this case there is no indication that, at any stage, such mobility data was de-anonymized or disaggregated, or that PHAC would, in fact, want to do such an operation, which would not be useful for large-scale public health purposes.

I think the issues in this case are fourfold or fivefold.

The first one is a very large-scale issue, which I think this committee will have to pay a lot of attention to, not just in this particular inquiry but also generally in the future, because, in some ways, as many have observed, this pandemic can be seen as a dry run for the slow-burning but increasingly intense and persistent emergency that is the global climate crisis. We are going to increasingly see surveillance measures at very large scales and with very large datasets being conducted for our own good. This justification will only increase as we enter deeper into a warming world. Massive data collection is already necessary to understand climate change, and this will be supplemented by equally massive data needed to mitigate it and to change state, corporate, population and individual behaviour. The big question we're going to have to ask here, but also increasingly in the future, is this: Is this necessity justified by the emergency situation?

The second area is transparency. I know that Dr. Parsons is going to look in more detail at some of these issues, but I want to mention that transparency is really key here. The biggest problem I see in this whole debacle is a lack of coherent communication and transparency by all levels of government involved. None of the parties involved was as transparent as it could have been. I would like to see greater transparency at every stage of this kind of process. This is linked to the question of accountability.

Accountability in this case, of course, is a role that is fulfilled largely by the federal Office of the Privacy Commissioner. It seems clear, from what the commissioner himself has said in the evidence he's given, that he was not consulted to the degree that he would have regarded as being meaningful or important.

I don't want to recommend any very specific changes to either the Privacy Act, for the government information, or PIPEDA, for the private organizations involved. Rather, I would say that both of these acts are now out of date and need massive and general reform, if not abolition and new acts put in their place. I would like to see something along the line of the EU's general data protection regulation but with greater attention to the varieties of privacy.

Consent is a key issue here too. I think it's clear that consent was not, in any way, involved in this data being used in the way that it was, but I also think that it's probably impossible for informed consent to be involved in a lot of these large data collection operations. Informed consent, sometimes termed “meaningful consent”, is virtually meaningless. First of all, it's impossible to understand or read the policies that are created by corporations and government. Second, the particular kinds of operations, such as location tracking, are often hidden in the policy. Finally, the consent is not meaningful, because it's often needed to supply a service. In other words, if you don't get consent, you don't get the service. That is an offer you can't refuse, not a situation of informed consent.

● (1115)

There should, therefore, be meaningful opt-outs; however, I'm not quite clear how the kinds of ideas touted by the Privacy Commissioner could work in terms of—

The Chair: Thank you, Dr. Wood.

I'm going to have to go to Mr. Parsons now for five minutes, please.

Mr. Christopher Parsons (Senior Research Associate, Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto, As an Individual): Thank you very much for the invitation to appear.

My name is Christopher Parsons, and I'm a senior research associate at the Citizen Lab, Munk School of Global Affairs and Public Policy. I appear before this committee in a professional capacity to represent my views, and my comments are based on research that I've conducted at the University of Toronto Citizen Lab.

The earliest days of the pandemic were chaotic in terms of information that was communicated by all levels of government. One area of confusion arose surrounding the extent to which these governments used mobility data and for what purposes.

Here are a few examples. On March 24, 2020, the Prime Minister and Dr. Tam asserted that telecommunications mobility data was not being used by government agencies. In the March 23, 2020 announcement that the government was partnering with BlueDot, the Prime Minister's official comments did not refer to mobility information. This information was only available by reading press statements, such as from U of T. It was only in December 2020 that information that mobility information was being used appeared on the COVIDTrends website. There is still no indication of where precisely that information comes from.

I raise these points not to indicate that the government misled Canadians per se, but that the information environment was chaotic and is yet to be adequately corrected. To begin this correction, I suggest that the committee recommend that the COVIDTrends website be updated to make clear the specific sources of mobility data the government is using, as well as including an opt-out from Telus's “data for good” program and enabling individuals to opt out of BlueDot's collection of information. Further, the committee should recommend that Telus incorporate the opt-out mechanism into all of its customer portals, for both Telus and Koodo, in obvious ways so individuals know they have this option.

I now turn to the issue of using telecom and data analytics information for health surveillance.

A key issue before this committee is Telus's and BlueDot's collection of information and the disclosure of it to the Government of Canada. In the case of Telus, they transform the qualitative nature of the data upon repurposing information that might be used to technically service their network into a sellable data asset. In the case of BlueDot, it remains unclear just how and under what terms they obtained the data that was provided to the government. Together, the activities of these companies speak to the government's seeming willingness to receive mobility data without first confirming that individuals have meaningfully consented to such disclosures.

As such, I recommend that the committee propose a series of Privacy Act reforms.

First, the private vendors that provide anonymized, aggregated or identifiable information to government agencies should be mandated to prove that they have obtained meaningful consent from individuals to whom the information relates before it is disclosed.

Second, the Privacy Act should be updated to capture anonymous or aggregated information that is collected or received by government agencies. Aggregated and anonymous information can drive policies affecting individuals and communities, and these individuals and communities do not lose an interest in the data simply because it is anonymous. Programs using such information should be required to receive approval from the Privacy Commissioner before they launch.

Third, the Government of Canada, whenever it is receiving either identifiable or aggregated and anonymized information derived from individuals from private organizations, should be required to demonstrate that such information was collected by those organizations after the individuals meaningfully consented to the collection and disclosure.

The Privacy Act presently empowers the government to collect significant volumes of information without the explicit knowledge or consent of individuals. PHAC has not indicated a desire, need or intention to subsequently reidentify those datasets; however, it could change that policy tomorrow, given the current status of the Privacy Act. This is a problem.

I recommend the following.

First, that the committee propose updating the legislation to include necessity and proportionality requirements, which would compel government organizations to demonstrate that identifiable or anonymized information is required to fulfill a specific activity and ensure that the sensitivity of the data is proportional to the activity in question.

Second, that government agencies be restricted from reusing information that they have acquired, absent reacquiring an individual's meaningful consent for reuse where appropriate.

● (1120)

The Chair: You have one minute left.

Mr. Christopher Parsons: Third, that government agencies be required to ensure that meaningful consent is obtained before individuals are included in anonymized datasets, that retention limits be placed on these datasets, that reidentification attempts be strictly prohibited, and that the Privacy Commissioner be empowered to assess the proportionality of any anonymized dataset programs.

In addition to the aforementioned suggestions, in a brief that was submitted to this committee I provided additional details and recommendations, in particular pertaining to compelling private organizations to disclose how they handle individuals' private information.

Thank you for your time. I look forward to your questions.

The Chair: Thank you.

With that, we're going to begin the six-minute rounds. The time allocation has been moved. There will be a bell that will interrupt this panel, but we'll begin with six-minute rounds and deal with that when we come to it.

Go ahead, Mr. Kurek. You are first with six minutes.

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

First, let me thank the witnesses for coming and sharing their expertise with us. It's very much appreciated.

Dr. Lyon, I noted that you started off your opening statement by talking about the definition of surveillance. That was in stark contrast, quite frankly, to what Minister Duclos shared with this committee, but your comments seem to be consistent with those of some of the other experts we've heard from. Can you comment further on your feelings as to what Minister Duclos said before this committee in suggesting that surveillance was not involved?

Mr. David Lyon: As I said, the problem is that “surveillance” is heard in many different ways. You have the common public notion of surveillance as having to do with the ways in which police, say, would seek out or keep watch over some suspect, or, equally, intelligence services might do the same sort of thing. That requires identifiable information to be used for that kind of surveillance, and that is a form of surveillance.

As I pointed out, the Public Health Agency of Canada does surveillance too. They are doing public health surveillance. They're using the large datasets, as we've heard, and that, too, is surveillance.

My argument would be that we need to broaden our definition of surveillance to include such things. The definition I was using—any focused, systematic and routine attention to personal details for the sake of some purpose, such as influence, management, control or protection—serves as a definition that covers all the range of surveillance activities that we see today.

Increasingly, of course, as both my other colleagues have commented, the move over the last few decades has been toward using larger and larger datasets covering larger and larger groups in a population, and surveillance is being done at different levels, but my point really was that, at whatever level, there need to be very serious concern and specific regulatory changes to keep up with the changes in technology that allow for these different sorts of surveillance.

Mr. Damien Kurek: Thank you for that, Dr. Lyon.

In an article you shared comments with that was published in the National Post, you made comparisons between some of the surveillance that was done post-9/11 and some of the surveillance that has been done over the course of COVID. This really becomes a question of the mass scale at which data has been used for Canada's public health response.

I'm curious, Dr. Lyon: Does the large scale of PHAC's program raise concerns with you? I'll try to ask the other witnesses as well.

Mr. David Lyon: The large scale.... Well, as all three of today's witnesses pointed out, the intentions of public health surveillance are ones that I think we would all agree with, in that they are trying very hard to track what is happening within the pandemic to see where the virus is spreading in geographical areas and within which population groups and so on. It's a very important task, but the fact that it's an important task doesn't reduce the fact that there are risks entailed in it at every stage: from data collection through to data analysis and the interpretation and use of those data. At every point, there are difficulties.

What I don't think we should be underestimating is the character of those difficulties. Those difficulties also—rather like the simpler sense of surveillance as watching a suspect, for example—involve harms. There are harms at the individual level, but there may also be harms at the group level: questions of equity, questions of justice, questions of how a group is characterized and so on. The question of the scale really just requires that we look at the issues of scale with a view to their being understood and regulated appropriately.

● (1125)

Mr. Damien Kurek: Thank you very much, Dr. Lyon.

I have a question for both you and Dr. Murakami Wood. Do you feel that the safeguards and frameworks have been adequately shared with the Canadian public to be confident that their data is being used correctly?

I'm hoping to get both of your responses, so you'll have to be really quick.

Dr. Wood, go ahead.

Dr. David Murakami Wood: Simply put, no. I agree that most of this data was probably necessary. It was important for it to be used for public health, but at the same time, no, the safeguards have not been made public or accessible in an adequate way.

Mr. Damien Kurek: I appreciate that.

Could I just get a quick comment from the other two witnesses?

Mr. David Lyon: I agree with Dr. Murakami Wood's view.

Mr. Damien Kurek: Okay.

Mr. Christopher Parsons: Also, no information is currently available to make clear how data is safeguarded and—

The Chair: I hate to do it, but we really have to keep moving. There were only a few seconds left when he asked the question.

I'll go now to Ms. Saks for six minutes.

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

Thank you to all of our witnesses who've joined us today. Your opening statements were quite helpful in shaping our discussion today.

I'd like to start with Dr. Murakami Wood. Witnesses in our previous sessions, as well as expressions today, have been about understanding how important data is for creating evidence-based policy when it comes to public health, particularly in the pandemic that we're in. I agree with you that this is in some ways a dry run and a learning curve for many experts, not just here in Canada but throughout the world.

We've seen countries, municipalities and provinces trying to navigate this pandemic with deficits in data and trying to shore that up in working with good datasets, such as Telus's "data for good". We know from PHAC that they've used this data at the federal level. We also know countries like Australia, Spain, Germany, Argentina, Brazil, Columbia.... The list goes on and on.

Dr. Murakami Wood, in your opening statements you said that evidence-based policy needs datasets, and it can be a good thing. In this particular case, you felt there was no suspicion of individual surveillance. Could you talk, first, about the importance of a data-driven approach? Also, you said there have been concerns about whether depersonalized, aggregated data can be re-personalized, but your comments seemed to indicate that in the case of Telus's "data for good" that wasn't the case.

Dr. David Murakami Wood: Thank you for your question.

My comments here really relate to the increasing need for good-quality data to produce policy that's effective. We've seen that, whether it comes from open-source data, industry data, or data generated through specific research, which many of us who are academics are involved in, this data is increasingly necessary to build public policy.

You will recall that we had similar arguments around good-quality datasets a decade ago, in the arguments about the long-form census. On that occasion, while there were arguments being made about privacy and so on, most of us in the academic world were actually on the other side of the debate and arguing in favour of the long-form census because it provided important data that allowed us to make effective social policy. I think that's the importance of this sort of dataset.

As David Lyon said earlier, it does not mean there are no risks. It does not mean that data can just be used in any way that a government sees fit to use it. It does not mean that government does not have to account for data and how it is used or provide evidence of consent, as Dr. Parsons has said. I think those things are all very important.

The final thing I didn't get to in my opening statement, which is absolutely vital, is to expand on what Professor Lyon said about group harms. One key thing about large datasets is that hidden within these datasets are existing forms of bias and prejudice.

I'll give you an example. Say, in Telus's "data for good"—this is just made up, by the way—it was found that people in a particular suburb of Toronto were travelling further distances more often than other people in Toronto. You could easily assume from this data that these people were spreading the virus or were disobeying government instructions on travel. In fact, if you look into this particular suburb, you find it's a low-income place, largely Black and of ethnic minority. You have in this area people who have to travel to get to warehousing jobs or work in the gig economy, and the reason they're mobile and moving more often is precisely because they're under-privileged. Therefore, to stigmatize these people or to blame them for the virus spread would be to misread the social facts on the ground.

That's just one notional example, but it's very important to be able to understand not just the data as facts but the data in its social context. That's what I think is really vital when we talk about—

● (1130)

Ms. Ya'ara Saks: I do appreciate that. Thank you.

We have seen from the assessments that have been reviewed that we've been able to pinpoint where more information for public health agencies, both municipally and federally...were able to help communities that were struggling based on that kind of data. I think there are two sides to the coin of that useful data when it comes to particular demographic sets.

I'd like to move on to Dr. Lyon, if I may.

In this world we're in of anonymized data, can we have perfect anonymity? Is it even possible? We know the value of this data and what needs to be collected, but at the same time there is much discussion about the safeguard rails that need to be put in place, or that we're discussing here. Can we reach that perfect anonymity in having useful data?

Mr. David Lyon: As I said, I'm not a technical expert, but it does seem to me, from the evidence, that such a notion is very hard to actually obtain in practice. There are ways of taking care, and taking more care with data analysis especially. And don't forget that I mentioned each of the stages. It's not only the collection, the gathering of those data in the first place. The analysis is critical, and within those forms of analysis anonymity may also be compromised, right through to the uses of those data.

I have great doubts that there is a real sense of anonymous data.

Ms. Ya'ara Saks: I understand.

Then PHAC's statement that it did not—

The Chair: Thank you. You're out of time.

Ms. Ya'ara Saks: Okay. Thank you, Mr. Chair.

The Chair: With that, we will go next to Monsieur Villemure.

[*Translation*]

Mr. Villemure, you have the floor for six minutes.

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

I want to thank the witnesses for joining us this morning.

I'll start by asking each witness a quick question. We can then delve further into the topic.

Mr. Lyon, was the process described by Health Canada in this case fairly opaque or transparent?

[*English*]

Mr. David Lyon: The process that was described by Public Health Canada....

I'm not sure that I grasped the question, really.

[*Translation*]

Mr. René Villemure: Is this a case of transparency or opacity?

[*English*]

Mr. David Lyon: I don't think you can make a simple “one or the other” here. There are aspects of transparency, and there are aspects of opacity. Really, I think that question distracts us from the real issues in front of us.

The Chair: With that, I've just stopped your time, Monsieur Villemure. We have about five minutes left.

Bells are ringing. At this point, I will need unanimous consent to continue this meeting.

My proposal, if I do have everyone's consent, is to proceed and let Monsieur Villemure finish his round, and give Mr. Green his round. That will still leave us sufficient time to get to the chamber, for those members who will do so. If that's the will of the committee, then I'm going to proceed in that way.

Some hon. members: Agreed.

The Chair: We will continue.

You have five minutes and eight seconds, Monsieur Villemure.

● (1135)

[*Translation*]

Mr. René Villemure: Okay. I'll move on to another question.

Regarding the case at hand, several people have spoken to us about a worthy aim. You have all done so this morning. However, there's a tendency for some to downplay the significance of the risks or the choice of methods. Minister Duclos, like the Public Health Agency of Canada, seems to dismiss these risks out of hand. Yet they're real.

Mr. Lyon, you said that data collection is a form of surveillance. While we don't like the word “surveillance,” things are the way they are. I suppose that surveillance completely excludes the idea of consent.

[*English*]

Mr. David Lyon: Yes, consent is very difficult to obtain. Dr. Murakami Wood already pointed this out in his talk, and that seems to me to be exactly right, that the notion that we could somehow gain consent.... The notion of consent is really important. It's really significant, and there are particular ways in which it could be sought, as Dr. Parsons pointed out, but it becomes increasingly difficult to obtain consent in the current data collection, data analysis environment within which we're living right now.

[*Translation*]

Mr. René Villemure: I gather that just because it's difficult to obtain consent doesn't automatically make it impossible to obtain some form of consent.

[*English*]

Mr. David Lyon: Absolutely not. There needs to be much broader public education, as it were, so that we understand what we're doing when we supposedly give consent and when we actually give consent.

Yes, there is far more to be done here.

[*Translation*]

Mr. René Villemure: Okay.

Mr. Parsons, I gather from your remarks that Telus or BlueDot didn't seem to have considered the consent issue.

What are your thoughts on the Telus program in terms of surveillance?

[*English*]

Mr. Christopher Parsons: As I noted in the full brief I submitted to the committee, Telus and Babylon Health have been in situations in which the Alberta privacy commissioner found that simply agreeing to a privacy policy is insufficient and does not constitute consent.

The Privacy Commissioner of Canada and the guidance on meaningful consent identify a range of activities that private industries such as Telus could undertake. To date, as far as I'm able to tell, none of those methods have been clearly undertaken. As such, information has been collected without meaningful consent or first being approved.

[*Translation*]

Mr. René Villemure: Mr. Wood, you spoke earlier about whether there's a need for transparency and accountability. I think that all these measures are meant to maintain or increase trust.

In your opinion, could this case undermine people's trust in institutions to some extent?

[*English*]

Dr. David Murakami Wood: Yes. I think there are two reasons for this.

One of them is direct, in that the actions of the government itself, in this case, and Telus as a corporation do indeed lead the public to suspect that maybe something is wrong, and therefore decrease trust.

However, there are also indirect ways in which trust is being decreased here. I'm sorry to say it, but I have to ask members of the committee to take some responsibility here too—at least politicians in general, not individually. There's also a political aspect to this, where both media and politicians have been involved in hyperbole, an exaggeration, around this case for political gain. That's on both sides, by the way.

It doesn't help, either, when we get reportage that says 33 million Canadians are being tracked. People start to believe that it means their individual communications are under surveillance, when that is not the case. Some of the reporting and, indeed, some of the quotes I've seen from politicians have been very irresponsible.

There are different kinds of trust problems here, but certainly the government and Telus have also been involved in decreasing trust.

[*Translation*]

Mr. René Villemure: I simply thought that the challenge at the outset was to weigh privacy against public health and to create a balance between the two.

Yet, the further we proceed, the more I realize that partisanship and public health are being weighed against each other.

Do you also feel this way?

● (1140)

[*English*]

Dr. David Murakami Wood: As we know—and those of you who are in Ottawa will know especially well right now—partisanship and public health are unfortunately in a kind of death struggle right now on the streets of Ottawa. I don't want to comment any further on that, but I will say that we have had a big problem in the last year or two with partisan understandings of public health priorities.

I don't think it helps, and I think it has played into some of the ways in which this particular scandal is understood.

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

I will suspend the meeting quite abruptly—or I plan to—at the end of Mr. Green's six minutes.

Go ahead, Mr. Green.

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

I appreciate the opportunity for this intervention. Having these witnesses before us today has been really helpful.

I would agree; I'm less interested in fault-finding in this moment and more interested in finding systems-level and legislative changes to these symptoms. This case is symptomatic, as has been identified, of the larger current concerns under our Privacy Act.

What I'd like to do with the majority of my time is allow each witness about a minute and a half for their intervention to provide, with fullness, in whatever way they can, what they believe should be the reforms, improvements or key points, as it started to go down that line, on improving our Privacy Act. Your submissions will become, hopefully, part of the recommendations from this committee, and this is what I'm most interested in.

So, [*Technical difficulty—Editor*] Dr. Murakami Wood, and then go Dr. Lyon and Mr. Parsons. Whatever you don't add in here.... You can provide in writing whatever further remarks and recommendations you have to improve our Privacy Act, so they can be considered by our analysts when we open up the discussion on recommendations.

Go ahead, Dr. Murakami Wood.

Dr. David Murakami Wood: Thank you.

I'm going to completely defer to Dr. Parsons in terms of the specific reforms that might be suggested to the Privacy Act. He has made a much greater and more comprehensive study of these things than me.

However, I'm going to borrow the old 1960s situationalist slogan, “Be realistic, demand the impossible.” The impossible I want to demand is in fact the complete abolition of the existing Privacy Act and PIPEDA. I want to see an entirely new architecture for information, data protection and privacy to be built in Canada at a federal level—and maybe at a provincial level too, because we have wildly incompatible provincial legislation situations at the moment, as you all know.

That's my recommendation. Every time these kinds of things happen, at the base of the problem is the fact that we have this archaic and out-of-date system for understanding how privacy relates to society—

Mr. Matthew Green: Thank you. My apologies for the intervention. I just want to make sure that Dr. Lyon and Mr. Parsons have an intervention. We have only a very short time.

Go ahead, Dr. Lyon.

Mr. David Lyon: I'm not going to repeat the same comments. Dr. Parsons really has the best ideas on the actual changes that are required. However, I also agree that we need to do something far broader.

I would like to recommend that we spend more time considering how these things are done in other countries. As I mentioned in my comments, in the European Union there isn't a question about whether this is or isn't surveillance. You start with the notion of surveillance, which is very broad. Then you recognize that there are different aspects to it and different kinds of harms that could result and different kinds of social benefits that could result.

I think looking at how other countries operate would be very helpful, specifically the European Union. More than one of us has mentioned the importance of looking at what is happening there, because the way in which the law is being reinterpreted for the present data-focused age is really highly significant.

Mr. Matthew Green: Before we pass it over to Mr. Parsons, who can take the rest of the time, I would ask each of you—perhaps you would be able to submit your remarks to this committee in writing—for ways in which we can improve on the EU's general data protection regulation. It's always my intention that we have the opportunity as legislators to create global leadership in this regard, so I'd like for you to be bold and expect the impossible, demand the impossible.

Mr. Parsons, you've been identified by some pretty esteemed colleagues as being a subject matter expert. I'll leave the last two minutes to you.

Mr. Christopher Parsons: Thank you for the question.

In the brief I submitted to the committee, there are a number of specific recommendations that I make throughout. I won't and can't go through all of them right now. However, the first one that I think is important for the committee to remember is that the ETHI committee a few years ago actually did a study of the Privacy Act. They saw a number of esteemed experts come. They produced a report. I would recommend starting there to see what still resonates. I believe much of what's in there still does.

More broadly as it pertains to the current PHAC situation, I think it is important and essential that the Government of Canada, when it's obtaining datasets from private organizations, whether it be identifiable or de-identified data, whether it be aggregated or not, be able to demonstrate that meaningful consent was first received before that information was collected by those private entities and then shared with the government. The Privacy Commissioner of Canada should both be apprised of and be required to approve any and all such projects. Further, within the Privacy Act itself, there should be a requirement that privacy impact assessments are performed and are made public. Currently, that's not often occurring.

Shifting slightly to PIPEDA, one of the real problems here is that a series of private organizations collected information and subsequently disclosed it. That information was largely collected without the knowledge of individuals. Privacy policies don't work. They do not constitute meaningful consent. However, the Privacy Commissioner of Canada does have guidance as to what should be done. I believe there should be a requirement that this kind of guidance should be built into PIPEDA itself.

Furthermore, there will, of course, be situations where information is disclosed to government agencies and others. One way that Industry Canada has worked with industry in the context of law enforcement has been to recommend that private companies produce what are called transparency reports. I have more on this in my brief. I would argue that while that is a step in the right direction from several years ago, these reports are not mandatory. They should be; moreover, they should be more comprehensive. They should include not just law enforcement disclosures. They should also pertain perhaps to copyright information and, in this case, the sharing of aggregated and de-identified data, and to whom that is shared.

● (1145)

The Chair: Thank you very much, Mr. Parsons.

My thanks to all of our panellists.

Members, we will reconvene with the second panel after the vote.

Until then, we are suspended.

● (1145)

_____(Pause)_____

● (1225)

The Chair: Welcome to the second panel of our meeting.

Today's meeting had to be interrupted by votes, which of course is our first and primary responsibility as members of Parliament.

I would now like to welcome our witness for the second part of the meeting. We have Alain Deneault, professor of philosophy.

If we have a five-minute opening statement, then we should get a full round for our first four members, at six minutes each.

Take it away, Monsieur Deneault.

[*Translation*]

Mr. Alain Deneault (Professor of Philosophy, As an Individual): Thank you.

I'm a professor of philosophy at the Shippagan campus of the Université de Moncton, in the Acadian Peninsula. I teach ethics and environmental ethics courses.

I'd like to quickly provide five pieces of context.

First, as we know, the health policies surrounding COVID-19 have led governments to adopt freedom-destroying measures in terms of lockdowns, curfews and mandatory disclosure of medical information. These measures have led to the non-renewal of contracts or dismissals and to electronic surveillance. The scientific basis for these decisions has often been debated and challenged. This has given some people the impression that public authorities are taking advantage of, or even exacerbating, the health situation to give free rein to unconstitutional practices.

Second, the technological infrastructure required to produce more big data at a faster rate leads to an increase in harmful environmental effects. To produce the big data that we use so much today, we need industrial server farms that consume a great deal of electricity, not to mention the 5G network that we must soon "accept" and the increasing production of information technology products in Asia. This sometimes leads to water issues. There are serious consequences in terms of greenhouse gas emissions, the depletion of rare metals and water issues. These consequences don't in any way point to sustainable practices in keeping with solutions to the environmental challenges that governments have claimed to be addressing in recent years.

Third, the production of big data, which comes from what I'll quickly call GAFAM, meaning Google, Amazon, Facebook, Apple and Microsoft—you understand that I mean the entire computer engineering sector—also constitutes a legal impoverishment from the governments' perspective. These companies, which hold a technical monopoly over what they generate, very often end up making law through giant contracts that we must constantly accept when use the software "given" to us.

These private ways of legislating result in law on which many court decisions are based. As you know, when it comes to information technology, representatives of these large companies often advise you, members of Parliament, since they have the best technical knowledge.

Fourth, this commercial stewardship of big data in the midst of the health crisis has been largely profitable for the major information technology companies, or GAFAM. The profits of these companies have increased by tens of billions of dollars, at the expense of SMEs and workers, who are far more trapped by the situation resulting from the health policies than these major companies.

I'll focus on the fifth point, even though I have very little time left. We'll discuss it later. The production of big data is, in itself, a totalitarian device. It involves monitoring the behavioural reality of subjects and making it predictable, even controllable. We know that, when we can monitor 150 actions of Facebook users, we know them better than their relatives. When we can follow only 300 actions, we know them better than they know themselves. It's a manipulation tool that Cathy O'Neil summarized as "Weapons of Math Destruction."

● (1230)

I personally advocate, not that we regulate this sector and make it ethical or acceptable, but that we prevent its production at source. This should be done in the manner of war diplomacy where sometimes there is agreement to refrain from developing certain methods or processes.

The Chair: Thank you, Mr. Denault.

[*English*]

We now have Mr. Patzer, for six minutes.

Mr. Jeremy Patzer (Cypress Hills—Grasslands, CPC): Thank you, Mr. Chair, and thank you to the witness for his testimony here today.

Quite often, when we have an emergency.... We can look back at what happened with 9/11 and the level of surveillance and security at that point in time. We're now looking at the measures that are going on throughout this COVID-19 pandemic.

What are the risks here that, because of the extraordinary measures that we have gone through to collect all this data, the government is not going to relinquish some of the ways and means by which it is surveilling citizens? Are they going to let people revert back to normal? I guess this is kind of what we're looking for. Is there going to be a backing off in the amount of surveillance and the amount of data that's being collected here?

● (1235)

[*Translation*]

Mr. Alain Deneault: The risk issue is broad. The first mistake that one could make here—I am not saying that this is your case—and that should be prevented, would be to read things in light of a single criterion. We are not in a situation where everything is black and white. The issue is to look at several criteria and ask how much risk there is.

There may be risks in not using massive data, but we also have to take into account the fact that we are dealing with a totalitarian mechanism that consists in controlling people to such an extent and with such efficiency that we even make them susceptible to manipulation.

The risk is to trivialize surveillance and make it a management technique that we have reduced to an almost technical modality, without gravity. This is what we have been doing for the last two years because of the emergency situation. In fact, we renew the health emergency from 10 days to 10 days, in discrete periods, without justification.

There will come a time when we will extend the scope of these so-called emergency measures to citizens who will be deprived of their constitutional rights. We cannot treat lightly the fact that we can have information about people on the grounds, for example, that they have not been vaccinated—which is a constitutional right, by the way—or that they are participating in demonstrations, which also are constitutionally protected, in principle.

Therefore, the perceived risk is to generate a mechanism that, in the name of technical management, allows for an unconstitutional attitude, measures and processes.

[*English*]

Mr. Jeremy Patzer: I feel like we're getting very close to a threshold here of infringing too far into people's lives, and the data people are generating, their own data, is being used against them.

Is there an ethical concern about the use of this data?

[*Translation*]

Mr. Alain Deneault: In my opinion, the problem is the mechanism itself. It is inherently totalitarian. To monitor people's every action, every move and every purchase, to cross-reference that data, and thus make it so that we know these people better than they know themselves, is a problem right from the outset. It is the very possibility of generating this amount of information that we should be mobilizing against.

I'm not going to give you a lot of bibliographic data. However, look at the thickness of this book written by Marc Goodman, a former Interpol and UN employee. In it, he sums up the technological crimes linked to mass data. I invite you to read this book, *Future Crimes*, the original version of which is in English. It shows to what extent the citizens of states that are no longer states governed by the rule of law when they allow this data to be collected and used, are structurally at risk of falling into an order where control is total.

I would have an example to give you, but I will let you ask a question so as not to monopolize your time.

[*English*]

Mr. Jeremy Patzer: Maybe you could give that quickly, and then comment really quickly as well on consent. Are people able to very clearly give consent to their data being used or taken?

[*Translation*]

Mr. Alain Deneault: Thank you for asking me this question. The answer is no, quite simply. Studies have been done on how difficult it is to really understand the contracts we are made to sign when we become users of these software programs that collect our data the moment we use them. We all know the saying: when we are given something such as software, it is because we are the product. It takes a legal background, and then some, to make an informed judgment about what we are signing up for when we use this software.

In any case, today, if you want to work and organize yourself socially, these instruments are coercive. Either you live in your basement and don't leave your house, or you use them, because society demands them. The issue, basically, is letting a totalitarian device unfold without any form of control and trying, after the fact, to patch things up in frameworks that will always be shaky, because the mechanism itself is problematic.

● (1240)

[*English*]

The Chair: Thank you.

Now we will go to Ms. Khalid.

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

Thank you to the witness for his testimony today.

Perhaps I'll start by reframing the questions that have been posed so far. With respect to how in this specific instance that data was used, we have heard from various witnesses throughout the study so far that balance needed to be created in order to have those COVID restrictions, for example, be properly applied in a good way, in one that restricted that infringement upon people's rights.

To our witness, would you agree that this mobility data helped us to better understand how people were moving and to better implement policies that protected people's health and safety, while also ensuring that their rights were protected as much as they could be?

[*Translation*]

Mr. Alain Deneault: First of all, to the question itself, I would like to answer with a question that explains the confusion in which we find ourselves as citizens faced with this mechanism: who can answer this question?

Who can know if this data is used in a fair way? Who controls it? Are the bodies that have access to this data not using it for purposes other than those for which it was intended to be used in the context in question?

We don't know. There is an opacity that arises at some point, ultimately, and no citizen has the time to check that out.

So we are strictly bound by relationships of trust. Whether we trust these entities or not, in the first instance, we cannot verify that. Secondly, the question that arises here must be broader. I insist on this, ladies and gentlemen. The question cannot simply be about one tiny use, it must be about the mechanism and all its possible uses.

[*English*]

Ms. Iqra Khalid: Thank you. I appreciate that.

Understanding the complexity of this whole conversation and this issue, I really hesitate to go down the path of whataboutism and philosophically talking about what the possibilities are, what the best practices are or what that perfect scenario is.

I've heard members and witnesses compare this to the 9/11 situation. In this instance, we're talking about a government using data to really protect and to develop COVID health policies for our nation, whereas, as we go down this path of more complex data and data production, as you mentioned in one of your five points, there is this role that private companies play that was not there with 9/11.

Can you compare, as our member talked about, what the distinction is between a government using this data and restricting a government's use of this data versus private companies doing so? What role does a government have to play in ensuring an adequate balance in the use of data?

[*Translation*]

Mr. Alain Deneault: First, I would like to play down the situation.

For at least a year, we have known that the COVID-19 pandemic is not comparable to the pandemics that struck down a third or half of the population in the Middle Ages. Indeed, this has been officially established by several countries in recent weeks.

We are dealing with a disease that has very clearly, in the past few months, been behaving in a way that can be characterized as endemic. It is particularly serious for certain categories of people, for example those who are gravely ill or who are older, among others. Public policies should therefore be able to protect certain groups of people.

Personally, if I had to answer the question about the relevance of this research, this is what I would say.

First, the health system is underfunded; basically, that is the crisis. If the health system were not underfunded, we would be able to support and accommodate groups that are vulnerable to this virus.

Secondly, the problem is ecological. This is where we should invest and do research. It is an ecological problem because we are dealing with zoonotic diseases, as we have seen many of them since the beginning of the century. Ebola and H1N1, among others, are zoonoses caused by the loss of biodiversity.

We can always develop even more polluting—I said this earlier and I would not like us to forget it— and destructive techniques that create even more problems with regard to the causes of these epidemics. Furthermore, we must stop locking ourselves into advanced techniques, which are likely to be used by ill-intentioned entities, or to be used excessively.

● (1245)

[*English*]

Ms. Iqra Khalid: Thank you.

I have just a very short question.

I know you mentioned it a bit in your opening remarks with respect to private companies and big data being produced. Do you think government should be regulating that usage?

[*Translation*]

Mr. Alain Deneault: Yes, I think the government should ban it. It's hard to hear a statement like that, because it's not often made. Yet I think we should, as a precaution, make sure that this data...

[*English*]

The Chair: Thank you. We're out of time for this round.

Now we will go to Monsieur Villemure for six minutes.

[*Translation*]

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

Good afternoon, Mr. Deneault.

I'm going to ask you two questions and I'm going to give you time to answer them in the six minutes I'm allotted.

Until now, the government side has often told us about the benefits of the end purpose, regardless of the premise itself. You have talked about banning the production of data, for example. People have said that there are benefits, without regard to the rest. The situation is trivialized. In fact, the Minister of Health was evasive when I put the question to him.

In the Monde diplomatique, you talked about mediocracy. You have in fact published a book entitled *Mediocracy: The Politics of the Extreme Centre*. You assessed the topic based on the following elements, among others: education, economy and culture. You mentioned that there was a loss of critical thinking.

Do you believe that this loss of critical thinking is also operative in government?

Mr. Alain Deneault: Critical thinking means trying to identify the ideological motivation for everything we are offered.

Why are we being offered such and such a thing?

Maybe, indeed, there is a benefit to using this data if it is done in a surgically relevant way. Let's face it, it's like putting a lid on a boiling pot. You're trying to control a mechanism that wasn't created to allow the Canadian government to deal with an epidemic. That's what critical thinking is all about, trying to identify the ideological motivation of products and social modelling. A mechanism has been created that allows for surveillance, that allows for control, that allows for predictability and manipulation.

I lived in East Germany. I saw people who could, if they wanted to, access the files that the Stasi had compiled on them. These files contained all sorts of entries, including telephone tapping and so on, like tailing of citizens who were considered to be undesirable elements of society. The people who had access to their Stasi files were terrified. Yet these files were nothing compared to what Google, Microsoft and Apple know about us. The Stasi files were nothing compared to that.

Today, if people can get access to the harvested data... I can tell you that it happens. Sometimes lobbyists go to public decision-makers and show them what they know about them. It's not pleasant.

When you find yourself in that kind of situation, then you think that there may be a tiny percentage of relevant uses that you can make of these instruments, but are they essential to those uses? I don't know, but I doubt it.

In any case, we cannot avoid asking the question in a general way. Today, there are a considerable number of books on this subject. As you can see, I've collected some myself, and I'm not working on that. They're all books criticizing the hold of digital technology on our lives, which dispossesses us intellectually and rationally.

● (1250)

Mr. René Villemure: Do you believe that this kind of situation is likely to erode public confidence or trust in government institutions?

Mr. Alain Deneault: It's interesting, because on COVID-19 and health policies, there have been two ethical discourses. I refer to documents from the Quebec government on trust and transparency. In these government documents, which are written by in-house ethicists, they say that for there to be trust, there must be transparency. Yet, at the same time, the message must be unique enough and unassailable enough to be accepted by minds that might capsize if the science were called into question.

Science thus holds a discourse that is supposed to generate confidence. In the case of the health crisis, we are always told about science and public management methods to generate confidence, but this is only achieved if there is no evidence that causes doubt. When measures are presented, we are informed of their benefits and told that, since we have been informed, we must believe in those benefits.

These same ethicists say we need transparency. People feel they have all the conclusive evidence to trust what they are told. However, officials should not say too much. That's what this document says. I could send it to you, if you like, for the committee's work. I am on page 15 of the Quebec government document entitled “Cadre de réflexion sur les enjeux éthiques liés à la pandémie de COVID-19”.

Mr. René Villemure: Since we only have a minute left, I'll go back to critical thinking. You know I have ethical reservations when I see what happened at the Public Health Agency of Canada, and when I look back at the WE Charity case and the Aga Khan case.

Is critical thinking still operative, or on the contrary, are we drifting towards a mediocracy?

Mr. Alain Deneault: Mediocracy is sticking to the behaviour of the average manager. Managers do what they have to do because they feel they have to. We are, in a way, caught in a kind of encompassing game, where we dare not question the ins and outs of a problem. Above all, once again, we have to think precisely, acutely and demandingly about the interests that are at stake when a situation arises.

Critical thinking is very much, in history, the relationship of citizens to power. Power usually promotes an ideology, that is, a perspective that is supposed to be operational and functional. It is the prerogative of power to administer things and to rely on documents that seem to be more relevant for making this or that decision. On the other hand, the opposition can engage in some critical thinking.

[*English*]

The Chair: I'm afraid we're out of time.

Now to finish us out for this panel, we go to Mr. Green for six minutes.

Mr. Matthew Green: Mr. Chair, I am sitting here in Hamilton Centre. I'll share with this committee that I had some concerns that we weren't perhaps using our best time at this committee in dealing with this particular case, given everything that's happening around the world, but in today's interventions and the study, particularly with this panel, I feel like we are seized with the question.

The question for me, what stuck with me, is Professor Deneault's reference to Facebook as a weapon of math destruction, understanding the ways in which AI can take big data and know people better than themselves and manipulate public discourse. I can only reference what's happening outside on Parliament Hill today, and in fact in cities across this country. I would say this is a very important discussion.

The professor acknowledged or at least referenced the idea of stopping production at the source, agreeing to stop developing certain types of tools. He talked about the way in which big data, ranging from mobility to social media and other surfing habits online, could lead to compromised democracies. I think about Pegasus, which is the spyware developed by the Israeli cyber arms company NSO Group, which is known to be used by countries around the world to compromise people.

My question for Professor Deneault is one that I've asked in the past: What major philosophical or sociological considerations that have arisen in Canada as a result of the COVID-19 pandemic should the federal government take into account when making decisions that impact Canadians' privacy? I would go further and allow him to elaborate on—in a broader sense, given this moment we're in—what measures we should be taking to safeguard people against the possibility of AI manipulation and other ways we can be compromised in our democratic processes and discourse.

● (1255)

[*Translation*]

Mr. Alain Deneault: Thank you.

I will quickly address two points. The first is that of informed consent.

When you find yourself in an emergency situation, a crisis—which I think is exacerbated in the case of the health crisis—you tell yourself that you have no choice.

You have to do this or that. You don't even have to consider your rights, or opposing views. Yet critical thinking would be to give voice, in the media in particular, to dissident scientists as much as orthodox scientists. Many virologists, epidemiologists and medical professionals have taken issue with government measures. The state makes decisions, and that is normal, it is its prerogative. However, it is not normal for society to have to march in step to the point where it loses its constitutional rights in matters of health decisions, and in particular with regard to vaccination and the vaccination of children. There is a lot of pressure. Being free and consenting when making an informed decision is a fundamental thing.

For the second point, I refer to a book of very great importance, Hans Jonas' “The Responsibility Principle”. Mr. Jonas is a great ethicist. He says three important things, which I will summarize at speed.

First, the data-generating techniques being implemented today, such as those of GAFAM, are not just likely to matter socially; they affect human beings intrinsically, both medically and culturally. Today, techniques are so powerful that they act on human subjectivity itself. Today, we create subjects that are not the same as in the days of the book, given the impact of social media, especially on young minds—I'm thinking of adolescents—that leave considerable, lasting traces.

Second, ethics must allow for predictability and measurement. We must be able to measure and predict the impact of discoveries, otherwise we are not being ethical and I don't think we are being democratic either. If we allow such techniques to be deployed on a societal scale, without ever being able to measure and control their impact, that is to check what they generate on a social and political scale, we are not being ethical; we are just doing a type of small-time management.

However, it is very important to be creative. Hans Jonas ends his plea by stating that ethics need to be creative. We have to be as creative as the technicians who, year after year, keep throwing gear at us that we didn't ask for.

[*English*]

Mr. Matthew Green: Mr. Chair, I'm going to allow the professor to close with the last 30 seconds here, with a request that.... Considering what the discourse has been in previous studies, what I am looking for, again, is trying to find the systems changes.

We're talking about our Privacy Act. We have opened up a discussion on our Privacy Act, so I would ask if the professor would be willing to, after this meeting, consider from his perspective the ethical considerations of our Privacy Act as it stands, as well as any international considerations that might be added as recommendations as we move forward.

It is my focus throughout this study to come from this committee—

The Chair: You have left him a lot less than 30 seconds now to answer.

Mr. Matthew Green: No, I don't need him to answer. I just want it in writing, Mr. Chair.

The Chair: My apologies. Carry on.

Mr. Matthew Green: If he could contribute those thoughts in writing, we could use them for our analysts, and for the good and welfare of this committee.

Thank you.

The Chair: We are now out of time.

Thank you very much, Professor, for your remarks.

The meeting is adjourned.