HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

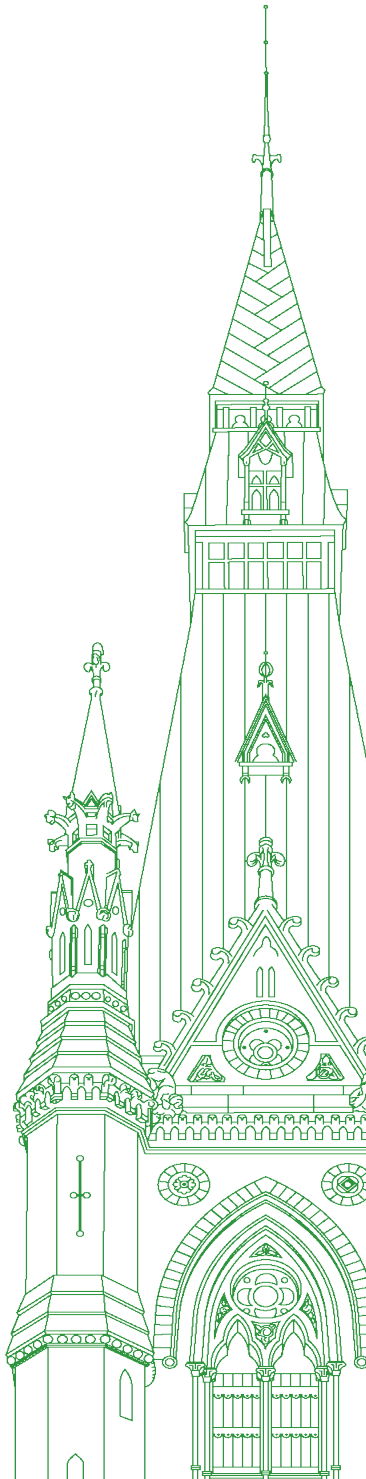
43rd PARLIAMENT, 1st SESSION

Standing Committee on Industry, Science and Technology

EVIDENCE

NUMBER 019

Friday, May 29, 2020



Chair: Mrs. Sherry Romanado

Standing Committee on Industry, Science and Technology

Friday, May 29, 2020

● (1400)

[*English*]

The Chair (Mrs. Sherry Romanado (Longueuil—Charles-LeMoyne, Lib.)): Good afternoon everyone. I call this meeting to order.

Welcome to meeting number 19 of the House of Commons Standing Committee on Industry, Science and Technology.

Pursuant to the order of reference of Saturday, April 11, the committee is meeting for the purpose of receiving evidence concerning matters related to the government's response to the COVID-19 pandemic.

Today's meeting is taking place by video conference, and the proceedings will be made available via the House of Commons website.

I'd like to remind members and witnesses to please wait until I recognize you by name before speaking. When you're ready to speak, please unmute your microphone and then return it to mute when you have finished speaking. When speaking, please speak slowly and clearly so that the translators can do their work.

As is my normal practice, I will hold up a yellow card when you have 30 seconds left in your intervention, and I will hold up a red card when your time for questions has expired.

Today we have two separate panels. For the first panel we have with us today, from the Office of the Privacy Commissioner of Canada, Mr. Daniel Therrien, Privacy Commissioner; Mr. Gregory Smolynec, deputy commissioner; and Martyn Turcotte, director, technology analysis directorate.

Before we start with the witnesses, I believe Mr. Masse would like to speak.

Go ahead, Mr. Masse.

Mr. Brian Masse (Windsor West, NDP): Thank you, Madam Chair.

I have a quick point of order related to committee business.

I'd like to move the following motion to continue our work with fraud protection in Canada. The motion reads:

> That all evidence and documentation received in relation to the subject matter of Fraud Calls during the committee's study of the Canadian Response to the COVID-19 Pandemic, be also deemed received by the committee in the context of its study on Fraud Calls in Canada.

This would allow us to fold in the work that we had on fraud into our previous meetings, which is relevant. I know there have been discussions with the parties to hopefully proceed in this fashion.

I move the motion and would ask for consent for that to pass, please.

The Chair: We have the motion on the floor.

Hon. Michelle Rempel Garner (Calgary Nose Hill, CPC): Madam Chair, on this point of order, because I'm a stickler for procedure, while I support Mr. Masse's motion, it is being moved on a point of order, and you would require unanimous consent for this to be moved.

I'm looking at the clerk in the gallery view. I want him to rule on that so that we can make sure we're setting precedent appropriately in this format. I have no problem with the motion, and I would support unanimous consent for it to be moved on a point of order, but I just want to do things by the book.

● (1405)

The Chair: Ms. Rempel Garner, I was just about to let him know that you cannot put a motion forward on a point of order, so you jumped ahead of me. Thank you, we're on the same page on that one.

With that, I will rule that I understand he was just going to table the motion and adding on that point of order was just an addition. I will rule it acceptable.

With that, I'll open the floor to debate if there is any.

Hon. Michelle Rempel Garner: I'm looking at the clerk. On a point of order with regard to procedure, perhaps Mr. Masse should just seek unanimous consent for this to be moved on the point of order, and then we have everything good to go.

The Chair: I've verified with the clerk and it's actually the chair who rules, not the clerk, and he should have not included the words “point of order”.

With that, we have the motion on the floor. I want to double-check if there is any debate. Otherwise, we'll go to a recorded division.

I see an analyst waving at me.

Mr. Francis Lord (Committee Researcher): I would request some clarification from Mr. Masse.

You talked about evidence regarding fraud calls that was received on May 20. There was much evidence on May 20 that was not related to fraud calls per se, but to fraud related to COVID-19, some of which was delivered through calls, many through texts or the web.

Is it specifically just fraud calls or all fraud related to COVID-19?

Mr. Brian Masse: It's COVID-related fraud. I don't believe I actually said a date. If I did, I apologize.

It's related to the evidence and testimony. I can leave that to you to determine. It's the evidence from the special hearings folded into the previous work that we did.

The Chair: Thank you, Mr. Masse, for the clarification.

Seeing as there is no more debate, we will go to a recorded vote.

(Motion agreed to: yeas 11; nays 0)

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

We will now go to our witness testimony.

Mr. Therrien, you have seven minutes to present.

[*Translation*]

Mr. Daniel Therrien (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): Thank you, Madam Chair and committee members for your invitation to discuss tracing applications, one of the approaches being studied in Canada and elsewhere to ensure a safe return to a more normal life. Please note that the expression “tracing application” is used in public speech to describe various mobile applications that serve as public health tools. Some applications are designed for conducting true contact tracing, while others have the goal of informing users and giving them advice based on their level of risk. The goal of an application is important for privacy purposes.

During this public health crisis related to COVID-19, the health and safety of Canadians is a key concern. It's natural for governments and public health authorities to try to find ways, including technological means, to better understand and control the spread of the virus. In this context, the Office of the Commissioner has adopted a flexible and contextual approach in its enforcement of privacy laws. We strongly believe that it's possible to use technology to protect both public health and privacy. Technology in itself is neither good nor bad. Everything depends on how it's designed, used and regulated.

When properly designed, tracing applications could achieve both objectives simultaneously, in terms of public health and the protection of rights. However, if implemented inappropriately, they could lead to surveillance by governments or businesses that exceeds public health needs and is therefore a violation of our fundamental rights.

● (1410)

[*English*]

I will now try to switch to English. I do not have the language button on my screen. I have a microphone and a camera, but no indication of language.

Does it work, even though I'm speaking English now?

The Chair: I believe it might be on the top right, Monsieur Therrien. There should be three dots.

Can we get verification that the interpretation is working?

Mr. Therrien, can you try to speak a few more words in English?

Mr. Daniel Therrien: Yes. I'm about to speak about the importance of the design.

The Chair: Unfortunately, the translation is not working. If you could hold on one moment, I'll stop the clock.

Mr. Therrien, we're just checking with IT. Because you're not switched over to English, when you do speak English, the translation does not come through. We cannot proceed until we verify that.

I'm going to suspend for one moment so that we can get IT to work with you.

● (1410)

_____(Pause)_____

● (1420)

[*Translation*]

The Chair: Mr. Therrien, you may continue your presentation, please.

Mr. Daniel Therrien: Madam Chair, I don't have the French version of the rest of the presentation. I suggest that my colleague, Mr. Smolynec, read the end of the presentation in English. I'll then answer questions in French, regardless of the language in which the questions are asked.

The Chair: That's fine. Thank you.

[*English*]

Dr. Gregory Smolynec (Deputy Commissioner, Policy and Promotion Sector, Office of the Privacy Commissioner of Canada): Good afternoon.

Following from the commissioner's opening remarks, appropriate designs of technologies, such as tracing applications, depend on respect for some key privacy principles recommended in the OPC’s “Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19”, and in a joint statement by federal, provincial and territorial privacy commissioners on contact-tracing applications.

In the interest of time, we will focus on six of these principles.

First is purpose limitation. Personal information collected through tracing applications should be used to protect defined public health purposes, and for no other purpose.

Second, these applications should be justified as necessary and proportionate, and therefore be science-based, necessary for a specific purpose, tailored to that purpose and likely to be effective.

Third, there must be a clear legal basis for the use of these applications and use should be voluntary, as this is important to ensure citizens' trust. Use should therefore be consent-based and consent must be meaningful.

Fourth, these exceptional measures should be time-limited. Any personal information collected during this period should be destroyed when the crisis ends, and the applications decommissioned.

Fifth is transparency. Governments should be clear about the basis and the terms applicable to these applications. Privacy impact assessments or meaningful privacy analysis should be completed, reviewed by privacy commissioners, and a plain-language summary published proactively.

Sixth is accountability. Governments and companies should be accountable for how personal information will be collected, used, disclosed and secured. Oversight by an independent third party, such as privacy commissioners, would enhance citizens' trust.

While governments have stressed the importance of privacy in the design of tracing applications, several of the principles I have mentioned are not currently legal requirements in our two federal privacy laws. For instance, nothing currently prevents a company from proposing an app that is not evidence-based and using the information for commercial purposes unrelated to health protection, provided consent is obtained, often in incomprehensible terms. A government could partner with such a company.

The current health crisis has made clear that technologies can play a very useful role in making essential activities safe. This meeting is about contact tracing, but potential benefits are much wider. For instance, let us think about virtual medicine or e-education.

What we need, more urgently than ever, are laws that allow technologies to produce benefits in the public interest without creating risks that fundamental rights such as privacy will be violated. Because of the growing role of public-private partnerships in addressing situations such as the COVID crisis, we need common principles enshrined in public sector and private sector laws.

Thank you. That concludes our statement.

● (1425)

The Chair: Thank you very much. With that, we will move to our rounds of questions.

Our first round of questions for six minutes goes to MP Rempel Garner.

Hon. Michelle Rempel Garner: Thank you very much to our witnesses, and thank you for your work in protecting Canadians during this time of crisis. I appreciate the framework you've put out proactively, with regard to privacy-related contact tracing.

Monsieur Therrien, are you absolutely confident that Canada's current privacy laws would protect Canadians if a privacy breach occurred in a contact-tracing app?

Mr. Daniel Therrien: No, I am not.

My office has been talking for several years now about the fact that our legal framework needs to be modernized and strengthened, and the current crisis clearly shows there will be a need to accelerate the technological revolution that was already at play before COVID.

Hon. Michelle Rempel Garner: Thank you.

Mr. Daniel Therrien: This acceleration requires an even stronger legal framework.

Hon. Michelle Rempel Garner: Has any federal government department actively engaged your office to work directly with regard to rectifying these laws ahead of a contact-tracing app being "strongly" recommended, as the Prime Minister said in a press conference last week?

[*Translation*]

Mr. Daniel Therrien: Perhaps I should respond in French, given the interpretation issue that we've encountered.

Hon. Michelle Rempel Garner: That's fine.

Mr. Daniel Therrien: The government hasn't consulted us regarding any tracing applications as such. People from the government put us in touch with members of the Mila research institute. We've given advice to people from this institute, upon their request, regarding their application's compliance with federal legislation. However, we haven't had any discussions with the government and we haven't had to give the government advice regarding an application or the applicable legal framework. This doesn't mean that we won't be approached.

[*English*]

Hon. Michelle Rempel Garner: Has the government given you any indication that they intend to accept the framework that you have recommended with regard to a privacy framework needed prior to a contact-tracing app being recommended by the federal government?

[*Translation*]

Mr. Daniel Therrien: We discussed the framework for tracing applications with government officials. They told us that they want to work within this framework. However, they reminded us that our assessment framework went beyond the current legislation in some respects, which is true, and that, ultimately, the government would need to comply with the legislation. They implied that some of the principles in our assessment framework may not be enforced because these principles went beyond the current legislation.

● (1430)

[*English*]

Hon. Michelle Rempel Garner: Mr. Therrien, given that you've spoken out about the lack of strength in Canada's privacy law as it stands, do you feel that it would be accurate to say that if a government strongly recommends the use of any contact-tracing application at present, Canadians would be asked to choose between their privacy and public health outcomes?

[*Translation*]

Mr. Daniel Therrien: I wouldn't go that far. I'd say that the legal framework should be improved, particularly in the context of COVID-19. As we said in our presentation, it's reasonable to believe that an application designed properly according to the principle of privacy, which we've argued for, can properly protect privacy while protecting public health. The legislation should be amended, but—

[*English*]

Hon. Michelle Rempel Garner: Given that the Prime Minister has said that he's about to strongly recommend a contact-tracing application, how confident are you right now that any application that's developed would be delivered in that ideal world you just spoke about, with stronger legislation for privacy?

[*Translation*]

Mr. Daniel Therrien: I think it may be a little too early to draw conclusions. It would depend on how the application in question is designed. Again, the government hasn't directly consulted us regarding any application. However, we'll be able to answer your question once we've had the chance to look at the design of the proposed application.

[*English*]

Hon. Michelle Rempel Garner: Are you concerned that the government hasn't contacted you proactively with regard to this? One would think they should be proactively working with your office, if the design is contingent upon privacy laws being respected in Canada, as you just put it.

Is the design contingent upon privacy laws being respected?

[*Translation*]

Mr. Daniel Therrien: We offered our services. Of course, it would have been better if the government had already started consulting us regarding the design of an application. We're hearing officials and ministers talk about the number of stakeholders involved, including the provinces. The government may not yet be ready to consult us.

The Chair: Mr. Therrien, sorry, but we're out of time for this round of questions.

[*English*]

We will now move to MP Erskine-Smith.

You have the floor for six minutes.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thanks very much.

Commissioner, it's very good to see you again. I too believe that the government should proactively consult with you in the development of these applications, and certainly so, as the government is leading the way, in partnership with the provinces, in the development of them. I think it's really important.

I want to ask about the principles you espouse. When I go down the list, I agree with almost every single one. I look to the purpose limitation, and of course that makes sense. I look to the idea that the collection of data has to be necessary and proportionate to the matter at hand, and that of course should be a key restriction. I agree there has to be a clear legal basis, and I want to get back to that. I agree with a time limitation, as well as with transparency, accountability and oversight. I think your office should be involved in oversight.

You talk about the need for a clear legal basis. In your joint statement with other privacy commissioners, and then again here today, you have indicated that it should be consent-based and entirely voluntary.

I wonder what you think about opt-in versus opt-out. If we didn't have an opt-out system and were only looking at opt-in, would opt-out be sufficient in the circumstance where if we didn't have an opt-out system and were only looking at opt-in we couldn't get the adoption rate necessary for the system to work at all?

● (1435)

Mr. Daniel Therrien: To be clear, in your question you've correctly put the question of legal basis, consent and voluntariness.

[*Translation*]

Under the Personal Information Protection and Electronic Documents Act, consent is required.

However, if the application is used by provincial governments, such as provincial public health authorities, consent may not be legally required. That said, my provincial commissioner colleagues and I are recommending consent—so it will be voluntary—mainly to boost people's trust in the application. People may not trust an application that doesn't let them choose whether or not to give consent.

[*English*]

Mr. Nathaniel Erskine-Smith: I agree that there needs to be trust, and it think it should preserve privacy in every possible way. I agree with the principles you have put forward. However, as it relates to protocols, whether it is the DP-3T or the TCN, I think there are other ways we can preserve privacy.

I do wonder, though. In your statement you said that de-identified or aggregate data should be used whenever possible, unless it will not achieve the defined purpose. If I take that same approach, then we're going to abide by these ideas unless we have to say, on balance, that in the public interest overall, the app won't achieve the defined purpose if we have an opt-in system only. If, instead, an opt-out system would get the adoption rates we need, would you be opposed to that?

Mr. Daniel Therrien: I'm not sure how that works in practice.

Mr. Nathaniel Erskine-Smith: I asked Google, as an example, at our committee the other day if the app could be put on individuals' phones by way of an OS update and if people would have the choice of whether or not to do that, but it would be effectively automatic and then people could choose to opt out. That could be one way of doing it.

[*Translation*]

Mr. Daniel Therrien: Basically, people will have the choice to travel, to move around in society, with or without a telephone. This brings us back to the fact that, in practice, if not legally, it seems that the voluntary use of the application and consent are necessary. They are also necessary to create a certain level of trust.

[*English*]

Mr. Nathaniel Erskine-Smith: Because I have only a few minutes left, can you give our committee an update on your efforts to take Facebook to court?

Mr. Daniel Therrien: Yes, I'll have to be careful, obviously, because we are before the Federal Court on this issue.

[*Translation*]

After completing the investigation report in spring 2019, we took the matter to the Federal Court of Canada in early 2020. We basically asked the Federal Court to order Facebook to comply with our recommendations.

As you know, under the current legislation, we don't have the power to require Facebook to accept our recommendations. That's why we took our request to the Federal Court in early 2020.

Facebook decided to file a motion to quash our request in Federal Court. Our request that the Federal Court order Facebook to comply with our recommendations and Facebook's motion to quash our efforts are therefore currently before the court.

● (1440)

[*English*]

Mr. Nathaniel Erskine-Smith: I'm running out of time, Mr. Therrien.

I previously indicated that I thought Facebook was breaking the law. They denied it, and it turns out that they did, in your view, certainly. I think that will be the view of the Federal Court.

I take the same view of Clearview AI and I encourage you to bring the full efforts of your office to bear against Clearview AI, which has clearly broken the law of Canada in relation to our privacy laws.

Thanks very much.

Mr. Daniel Therrien: Thank you.

The Chair: Thank you. We will have our next round of questions.

[*Translation*]

Ms. Gaudreau, you have six minutes.

Ms. Marie-Hélène Gaudreau (Laurentides—Labelle, BQ): Good afternoon, Mr. Therrien. I'm very pleased to be hearing from you today.

Mr. Daniel Therrien: Good afternoon.

Ms. Marie-Hélène Gaudreau: I'm very concerned about the public health and privacy challenge that we're facing.

I'm also a member of the Standing Committee on Access to Information, Privacy and Ethics. I'm very concerned about the possibility that any company could propose applications at this time.

We know that there are ways to anonymize and aggregate all the data.

That said, what specific legal foundations should we, as legislators, be prioritizing right now in this health emergency?

Mr. Daniel Therrien: In my opinion, we can proceed in two stages.

As I was saying, even under our current flawed legislation, if an application were properly designed, it could work.

That said, a group called CIFAR, a research institute mandated by Dr. Mona Nemer, the Prime Minister's chief science advisor, recommended specific legislation for tracing applications. This legislation would essentially replicate the principles adopted with our provincial colleagues, and would give the federal or provincial commissioners a monitoring role, a watchdog role, with respect to the implementation of these principles.

The legislation should be amended. I wouldn't say that it's necessary to amend it immediately, but in the near future. These amendments would address not only the tracing applications, but also other uses of technology that are necessary and very useful for society. Consider telemedicine, for example, which is increasingly being used in the context of COVID-19.

It's extremely useful for society to have this type of tool. However, what about the privacy of conversations between patients and doctors on digital platforms?

The legislation is completely deficient when it comes to protecting personal information.

Ms. Marie-Hélène Gaudreau: Exactly.

Mr. Daniel Therrien: The legislation must be amended soon, if not immediately.

Ms. Marie-Hélène Gaudreau: I gather that we're talking about the decorrelation of the social insurance number and about favouring a digital identification that will enable us to protect people's privacy. As you've already said several times, the personal data of 30 million out of 37 million Canadians is in circulation and can be used. Fraud makes this clear.

I want you to speak about the urgent need to address this. You've been telling the government about this issue for several years. Unfortunately, from one piece of legislation to the next, we keep moving straight past the issue.

What do you think about this?

Mr. Daniel Therrien: As you said, we've been suggesting for years that the federal legislation be amended. However, this issue is even more urgent in the context of COVID-19 and the increasing use of technology for purposes that are very useful but that expose people to risk. This is one of our important messages today.

You're talking about digital identity. That's one aspect. We've seen in the past that digital identity based on a social insurance number doesn't protect Canadians very well. This issue must be addressed as part of a legislative reform. That said, the issue isn't straightforward. Modern ways of protecting identity could be based on biometrics, among other things. However, the use of biometrics also raises privacy issues. This must also be addressed.

● (1445)

Ms. Marie-Hélène Gaudreau: Okay.

I now want to ask a question about the approach implemented at Statistics Canada to measure the level of trust. You also know that we have a very low level of trust with regard to the management of our data.

What do you think of the results, which will be released in July, concerning the trust that Quebeckers and Canadians have in the government, among other entities, and which could enable us to make quick choices?

Mr. Daniel Therrien: Are you talking about the results of our survey regarding Statistics Canada?

Ms. Marie-Hélène Gaudreau: I'm talking about the recently announced survey regarding people's level of trust, which is under way. The results will be released in July.

Mr. Daniel Therrien: I'm not sure that I saw what you're referring to. However, one thing that COVID-19 has demonstrated is that the private sector and the public sector are working together with regard to the use of data, which isn't necessarily a bad thing.

For example, we can see that the federal government and the provinces are holding discussions with various developers, including Google, Apple and many others. The private sector and the public sector are working together on data processing. Since data travels between the two sectors, this shows us that we should amend not only the private sector legislation, which has been discussed extensively at the federal level for years, but also the public sector legislation. It's very important—

The Chair: Sorry, but you're out of time.

[*English*]

Our next round of questions goes to MP Masse.

You have six minutes.

Mr. Brian Masse: Thank you, Madam Chair.

Again, thank you to you and the committee for the motion passed earlier to help Canadians fight fraud. It's much appreciated.

I will start with this question. In 1983, when the Privacy Act was passed and we created our current regime, we had floppy disks. We had mostly paper files, all those things. There hasn't been a major modification to the act. There were two attempts, I think, in 2010 or 2011, in which there was tabled legislation that Parliament never passed, so we're dealing with a very antiquated process to protect the public.

I believe the work the Office of the Privacy Commissioner has done since I've been a member of Parliament has been terrific. It's been important for citizen rights and also important for the economy. I would argue that it's actually strengthened investment in newer technologies in some sectors.

First of all, should this contact tracing be rolled out, would there be a way to differentiate where the exact strengths and weaknesses of an application could be within your powers? Second, would you be in support of a process whereby Parliament could reconvene quickly to pass legislation to give specific empowerment to protect people for data contact tracing? Would that be something that you would consider, as opposed to living with the weaknesses of the current legislation?

[*Translation*]

Mr. Daniel Therrien: Clearly, it would be much better if the legislation were amended. I spoke about the transfer of data between the public and private sectors. However, there's also the current issue of transfers between the federal and provincial governments. It's a very complex world, with a number of stakeholders. It would be extremely useful to adopt common principles for all stakeholders in order to better manage data transfers and data use while respecting privacy.

As things stand now, the Office of the Privacy Commissioner of Canada would have jurisdiction only if a federal department were using data. This possibility isn't straightforward, since the federal government says that it wants to favour an application that could be implemented by the provinces. If no personal information is collected by a federal institution or department, the office would have no role to play. However, if provincial authorities collect and use personal information for the purposes of COVID-19, then my colleagues in the provinces will have jurisdiction.

● (1450)

[*English*]

Mr. Brian Masse: Okay.

One of the things that you did was outline to us some major points. One weakness I'm concerned about and would like to get your opinion on is if we did contact tracing. It seems like a lifetime ago, but when Paul Martin moved to outsource the Canada census to Lockheed Martin—which was done—one of the problems that we faced, and fought a national campaign to reverse, was for the data to stay in Canada for assimilation because it was going to be shipped to Minneapolis, I believe, at that time. Under the U.S. Patriot Act, it became vulnerable.

Do you have any concerns about foreign applications and movement of data on any contact tracing? There have been considerable discussions internationally—including in France, most recently—about contact tracing, even everything from surveillance technologies.... You could even have consumer exposure. How do you feel about the data, information and security staying in Canadians' hands?

[*Translation*]

Mr. Daniel Therrien: I'll start by saying that Canada recently entered into trade agreements that limit its power to impose rules requiring that data remain in Canada. That said, some multinational corporations have their servers in Canada, which could be a solution, in practice. This issue is very complex. Trade agreements are a very significant factor that can limit Canada's power to require that data remain in the country.

That said, even if foreign companies had a role to play and even if personal information were to leave Canada, this wouldn't be an issue, provided that the companies comply with the proposed principles. Google or Apple could therefore say that they don't want to collect this personal information.

I'll conclude by addressing the “if.” If our principles are respected, there's no issue for privacy. However, companies or even the government are under no obligation to comply with the proposed principles. The Personal Information Protection and Electronic Documents Act doesn't go as far, which means that companies and the government could fail to comply with some of our principles because these principles aren't legally binding.

[*English*]

Mr. Brian Masse: Really quickly, the problem with your current circumstance is similar to Facebook. You have to go to court. You have very limited tools to enforce breaches and bad conduct. Is that not correct?

[*Translation*]

Mr. Daniel Therrien: That's certainly part of the challenge. As I said, our legal system doesn't include basic principles such as those that we proposed to regulate the collection and use of personal information through tracing applications.

[*English*]

The Chair: Thank you very much.

We will now go to MP Patzer for five minutes.

I have a quick reminder. When you see this yellow card, you have 30 seconds until the end of your intervention. Thank you.

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

I have a quick question right off the top here. Would it not be a violation of personal property rights to force an opt-out system for contact tracing, especially since it requires a forced update on our phones, which are our personal property, not the government's?

[*Translation*]

Mr. Daniel Therrien: Again, I am not sure I understand exactly how such a measure would apply in practice.

I understand that the companies responsible for the platforms could propose a modification that normally could or could not be accepted by the user. Are we talking about making the device not work unless consent is given? I'm not sure I understand exactly the nature of the proposal that would lead us to implied consent.

[*English*]

Mr. Jeremy Patzer: Yes, and again, it's the whole forcing of an update onto somebody's phone so it would automatically have that update. I get the consent piece, but for it to work in practice, you would have to force the system onto people's devices.

Moving on, recently an epidemiologist and associate professor at the University of Ottawa stated, “public health issues take precedence over individual rights issues”. Does your office share this belief that public health trumps individual rights?

● (1455)

[*Translation*]

Mr. Daniel Therrien: No, we believe that both of these objectives are very important. We do not in any way question the importance of protecting public health, especially at this time. We don't think it's a question of one interest over another. We think it is entirely possible to protect both interests at the same time.

[*English*]

Mr. Jeremy Patzer: Do you think the government is operating under the assumption, though, that public health takes precedence over individual rights?

[*Translation*]

Mr. Daniel Therrien: That's not what I'm hearing from ministers and public servants. What I am hearing is that privacy is very important, even paramount, according to some. I'm not questioning the interest or the intentions. Rather, I am questioning the fact that it is possible for certain players, including companies, to ignore the principles we are promoting and not protect privacy.

What I'm hearing are goals and intentions that I think are laudable. The question is whether they will be put into practice. That's why we are offering our services to look at exactly how these technologies would be designed.

[*English*]

Mr. Jeremy Patzer: Thank you for that. I appreciate it.

Has the government previously shown it is willing to fully co-operate with your office and its investigations?

[*Translation*]

Mr. Daniel Therrien: Departments generally cooperate with our investigations. They don't always agree with us. On balance, again, we do not have the authority to order a department or a company to behave in a certain way. Procedurally, departments cooperate, but on a fairly regular basis, not always, of course, departments do not agree with our recommendations.

This brings us back to the deficiency of the legal framework. We believe that a privacy expert should be able to order certain changes in practice to ensure that privacy rights are respected, as is the case in other jurisdictions.

[*English*]

Mr. Jeremy Patzer: On March 20, your office issued guidance on privacy and the COVID-19 outbreak, and stated that you will "protect the privacy of Canadians, while adopting a flexible and contextual approach in its application of the law". What does the commissioner mean by "a flexible and contextual approach"?

[*Translation*]

Mr. Daniel Therrien: On the one hand, in our compliance activities, we have less frequent contact. We are giving departments more time to administer the law. That's the procedural side. On the substantive side, some concepts can be interpreted in a more flexible way in the current context.

[*English*]

The Chair: Thank you so much.

Our next round of questions goes to MP Longfield.

You have five minutes.

Mr. Lloyd Longfield (Guelph, Lib.): Thank you.

Thank you, Mr. Therrien, for being with us today. You're giving us very important testimony.

I'm looking at the accountability principle. It mentions, "If effectiveness of the application cannot be demonstrated, it should be decommissioned and any personal information collected should be destroyed." On the question of effectiveness, I spoke with an epidemiologist today who was saying, because of the long gestation period of this virus, it's very hard to determine whether tracing would be effective.

How would we look at effectiveness of tracing as an example?

[*Translation*]

Mr. Daniel Therrien: That's an excellent question.

No one is claiming that tracking applications are a panacea or a silver bullet, neither the privacy community nor public health authorities. However, it is quite conceivable that tracking applications could contribute to the solution and help identify people who have COVID-19. More traditional methods could then be used to contact them and provide them with advice on how to stay home.

Applications will therefore not necessarily be the solution as such, but they can contribute to it. This is a context where we are facing a completely new phenomenon.

Privacy principles say that you have to be able to demonstrate the effectiveness of the measure, but that does not mean that you have to demonstrate absolutely that the measure is going to be absolutely effective. This is perhaps, once again, where we could have a flexible and contextual approach.

What we're looking for is a scientific basis. We're not trying to prove the effectiveness of the measure beyond doubt. It's about demonstrating that it can be effective with other measures.

● (1500)

[*English*]

Mr. Lloyd Longfield: That's very good. Thank you.

You mentioned public health. Of course, that's a concern with federal-provincial jurisdictions, and also transnational jurisdictions as people travel around the world.

I spoke with the Homewood Research Institute this week and we talked about the mental health apps that are out there. It has now developed a framework for measuring the effectiveness of mental health apps but is concerned about data and the protection of data, particularly on apps that might have been developed in other countries.

Do we have agreements internationally, or do we work with foreign-developed applications that would then have to meet Canadian regulations in order to be used in Canada? How do we share information across jurisdictions, either provincially or internationally?

[*Translation*]

Mr. Daniel Therrien: The protection of data on telemedicine applications or during the virtual provision of mental health advice, for example, is one of the reasons why we are of the opinion that the legal or statutory framework needs to be changed as soon as possible.

This does not mean that there is no law in force at the moment. Both public and private sector laws apply, but they are very deficient. I am not aware of any significant protections for confidential information that would be exchanged between patients and physicians.

[*English*]

Mr. Lloyd Longfield: Thank you.

I think our judiciary would be interpreting laws as context changes, and those interpretations would then be applied to future rulings as well.

[*Translation*]

Mr. Daniel Therrien: Yes. It is a well-known and well-accepted method of statutory interpretation to consider the context and purpose of the measure.

[*English*]

Mr. Lloyd Longfield: We're developing the digital strategy, the digital charter. I'm assuming you've been working extensively with the industry, science and technology groups around digital transitions.

Is it fair to say we're into that process, or has that process yet to begin? Would that process help us in terms of what you're now working on in the COVID-19 cases?

[*Translation*]

Mr. Daniel Therrien: We have had discussions on digital strategy with the government and with the Department of Industry, among others, but these meetings are very irregular. We share the objective of these measures, to make better use of data and to have digital government, but we are not particularly consulted on this issue.

I'll take you back to the fact that laws need to be modernized to reap the benefits of digital government.

The Chair: Thank you very much.

[*English*]

Mr. Lloyd Longfield: Thank you.

The Chair: Our next round of questions goes to MP Dreeshen.

You have five minutes.

Mr. Earl Dreeshen (Red Deer—Mountain View, CPC): Thank you very much, Madam Chair.

We're certainly living in unprecedented times. That's true not only because of the impact of COVID-19 on the economy, but this pandemic has opened the door to unprecedented intrusion by governments into both the personal affairs and personal information of all Canadians.

Mr. Therrien, you mentioned in your remarks that what we need, more urgently than ever, are laws that allow technologies to produce benefits in the public interest without creating risks that fundamental rights, such as privacy, will be violated.

As you know, Parliament is essentially shut down at the moment, so who knows when it's going to return to the role of dealing with essential legislation—and, for that matter, why would it, when it's getting away with government-by-press-conferences? Yet, as has been noted, the current crisis heightens the need for law reform.

What are the dangers of moving forward with technologies such as contact tracing if stronger laws are not in place?

● (1505)

[*Translation*]

Mr. Daniel Therrien: I'll first talk about tracking applications, and then I'll come back to technology in a more general way.

As we explained, many of the principles we propose for tracking applications are currently not legally binding. This is the case, for example, with the principle that applications should only be used for tracking purposes in the name of public health. Nothing in the current legislation prevents a company from offering a tracking application and then using the information it obtains for commercial purposes. The only control that exists is the requirement to obtain consent under a privacy policy that we all know will be ambiguous.

I'll stop here regarding tracking applications to give you the opportunity to ask more questions.

[*English*]

Mr. Earl Dreeshen: I think part of it is that you have spoken in the past about the need for new laws and for us to get together to talk about it. I was on the privacy committee many years ago, when we were trying to make some changes. It's important for parliaments to be able to sit to deal with these types of things.

In terms of what you mentioned a few days ago, I'll just quote what you said: “I believe we have finally reached the point where the question of whether privacy legislation should be amended is behind us. The question before us now is how.” You mentioned how important it is for government to get on to this so that it has the legal framework to be able to work.

I want to give you an opportunity to emphasize how important getting the laws right, and getting them done right away, will be for Canada's privacy.

[*Translation*]

Mr. Daniel Therrien: I'll give some examples. Getting back to the tracking apps, I would say that a large part of the Canadian population will probably not be convinced that this information will be used properly, because people already don't trust the current legal framework. That in itself is a major problem. If the legal framework were more rigorous, it is quite possible, if not certain, that people would have more trust and would be willing to use this kind of application; they would see the public health benefit and would be less concerned about their privacy being violated.

Now let's move on to the issue of tracking applications.

The COVID-19 pandemic has caused the delivery of medical services, education and many other services to be delivered digitally and virtually. I think this will continue, although it may not be at the same pace as it is now.

These services are essential. Medical services, in particular, rely on confidential information protected by professional secrecy. Yet this data is currently exchanged on platforms with poor legal frameworks, giving people reason to fear that their confidential information will not be protected.

New technologies offer immense advantages. Just think of telemedicine or digital education. On the other hand, people's privacy needs to be protected by adequate laws.

[*English*]

Mr. Earl Dreeshen: Certainly. Thank you.

My time is just about up, but I certainly want to mention that if you look at Internet reliability in rural Canada, it's about one-eleventh as reliable as it is in urban Canada. That makes it very difficult.

Thank you very much, Madam Chair.

The Chair: Thank you very much, MP Dreeshen.

Our next round of questions goes to MP Jowhari.

You have the floor for five minutes.

Mr. Majid Jowhari (Richmond Hill, Lib.): Thank you, Madam Chair.

Thank you, Mr. Therrien.

Mr. Therrien, on May 7 of this year, the Privacy Commissioner of Canada and your provincial and territorial counterparts issued a joint statement in which you urged all levels of government to respect the privacy principles.

First of all, let me thank you for the great work that you and your department and your counterparts are doing on this front. I understand the federal government hasn't decided on any contact tracing. Have any of your provincial counterparts decided, or are they close to any decision, on a contact-tracing application?

● (1510)

Mr. Daniel Therrien: I may be out of date. Certainly in Alberta an application has been in place for some time now.

Mr. Majid Jowhari: Okay, great. Thank you. I was hoping you would say that.

Given the fact that Alberta has chosen to proceed with it, can you give us an insight into the alignment of the privacy criteria you have developed with the application features? Does this application meet those privacy requirements?

[*Translation*]

Mr. Daniel Therrien: The compliance with privacy laws of the application used in Alberta is currently under review by my provincial colleague, Jill Clayton. This issue is therefore on hold.

I would say, very summarily, that there is certainly an alignment of the conditions of use of this application with some of our principles, including the voluntary side. Consent is also required for the use of this application in Alberta. So one of our principles is being applied. Are they all? I will leave it to my colleague from Alberta to judge that.

[*English*]

Mr. Majid Jowhari: That's great.

Vis-à-vis Alberta, do you know the adoption rate in the province for that application?

Mr. Daniel Therrien: I'm afraid not.

Mr. Majid Jowhari: Okay.

How do you feel we would be able to achieve an adoption rate of anywhere from 60% to 80% without an opt-out model?

[*Translation*]

Mr. Daniel Therrien: That's an excellent question. Adoption rates in many territories are around 20%. Even if an application were mandatory, there would be ways for the population to get around that, such as not using a phone. This brings us back to reality. In my opinion, there has to be a voluntary side to the use of the application.

In this context, how do we increase the adoption rate? It would be by having conditions that foster trust. We need a system where privacy principles are accepted. I think transparency is also very important.

[*English*]

Mr. Majid Jowhari: Thank you. I have about two minutes left.

I want to go into the ownership of the data. As you know, there are discussions around centralized and decentralized models. What are your thoughts around the ownership and scope of the data that's being gathered, during and after the COVID-19 pandemic?

Could you make it brief, because I have a follow-up question?

[*Translation*]

Mr. Daniel Therrien: In general, decentralized systems provide better privacy protection. Having said that, we are not opposed to some centralized aspects, as long as the data is deemed necessary by a public health authority, such as knowing where the outbreaks are.

[*English*]

Mr. Majid Jowhari: That's perfect. Thank you.

In terms of deeming what data is necessary, as we are trying to move to the next stage, which is the predictive model that could help with wave two and wave three, don't you believe that maintaining a larger scope of data, as well as maintaining the data much longer, would give us a much stronger ability to do the analytics we need in order to get to that predictive model?

[*Translation*]

Mr. Daniel Therrien: The higher the adoption rate, the better for efficiency and data analysis. I agree with that.

In terms of the time during which the application will be used, one must realize that we are talking about particularly sensitive data that would not normally be collected. I'm not sure I agree with the use of this data over a long period of time.

● (1515)

The Chair: Thank you very much.

Mr. Savard-Tremblay, it's your turn, and you have two and a half minutes.

Mr. Simon-Pierre Savard-Tremblay: Thank you, Madam Chair.

Thank you too, Commissioner.

You spoke of the weaknesses in the law. You said there were gaps in the law and that things could be changed. There are provincial laws. Shouldn't we just rely on them?

Mr. Daniel Therrien: Data is moved around between administrations and between countries. Therefore, there is a need for strong laws in all jurisdictions, including the federal government. This is a factor that cannot be ignored.

Mr. Simon-Pierre Savard-Tremblay: Could you tell us a little bit more about the legislative changes that could be made? You say it could be in all jurisdictions. So you're not against the idea of provincial legislation as well. I would imagine it would be a federal law that would be more focused on coordination than subordination.

I'd still like to hear what you have to say about any changes that might be made.

Mr. Daniel Therrien: For the past few years, we have been proposing rights-based federal legislative reform. The principles of our assessment framework have been taken up in large part in our joint statement with our provincial colleagues. We are therefore talking about such principles, which are generally not in current federal law. They are a little more present in some provincial legislation, including the Quebec legislation, which contains the principle of necessity. However, according to my colleagues, provincial legislation also needs to be amended.

So we're basically talking about the principles set out in the joint statement, which should have the force of law, not only in my view, as a federal actor, but also in the view of my provincial colleagues.

Mr. Simon-Pierre Savard-Tremblay: That's perfect, thank you.

Madam Chair, how much time do I have left?

The Chair: You have 25 seconds left.

Mr. Simon-Pierre Savard-Tremblay: I don't think I'll have time, in 25 seconds, to—

Mr. Sébastien Lemire (Abitibi—Témiscamingue, BQ): Let me jump in and ask a question.

In concrete terms, to whom does medical data, such as a positive result to a COVID-19 test, belong? To the individual, or to the state?

Mr. Daniel Therrien: I don't think property law concepts are so applicable here. It's clear that privacy rights seek to give individuals significant control over their information, including their health information, although it may not be a proprietary right.

That being said, if an authority—

The Chair: I'm sorry, Mr. Therrien, but that concludes this round of questions. We'll move on to the next one.

Mr. Masse, you have the floor for two and a half minutes.

[*English*]

Mr. Brian Masse: Thank you, Madam Chair.

I want to go back a little bit on process. Early on, I was approached by a company that does contact tracing through malls and shopping. The way it works is that the government set up a process to stream any of those companies interested in doing work with the government through three portals of Industry Canada. It is actually a good model and it has done some great work.

Now, I don't know what happened with regard to that file, but from what I understand, there really hasn't been any follow-up with you or your office. It's been more than a month now, or closer to two months, and there hasn't been any robust discussion, which I want to confirm, about creating an app or maybe potentially screening any potential partnership with a company for a public-private partnership. I think part of what we would need satisfaction with, in order to ensure Canadians' privacy, would be that the company we're doing a partnership with would also go through a screening.

Mr. Daniel Therrien: Are you talking about a contact-tracing app?

Mr. Brian Masse: Yes, please.

[*Translation*]

Mr. Daniel Therrien: The only tracking application for which we were consulted in detail was Mila's in Montreal.

The federal government has no legal obligation to consult us. We offered our services. The government may have decided not to do business with the company in question, in which case it does not have to consult us, of course. We have offered our services and it is up to the government to accept them or not. The only application for which we were consulted was the Mila.

● (1520)

[*English*]

Mr. Brian Masse: Do you have any personal or professional feelings—more the professional feelings, I guess—about either a non-government agency like China or a private equity fund, where we have no idea who owns the company, working with Canadians' private data, versus a Canadian company with a Canadian app?

[*Translation*]

Mr. Daniel Therrien: There are gaps in the law. If data are to be properly protected in the current deficient framework, the trust that must be placed in the company becomes a particularly important factor. We should therefore stay away from less trustworthy companies, obviously.

[*English*]

The Chair: Thank you very much.

Unfortunately, that is all the time we have for this first panel.

With that, I will thank the Privacy Commissioner.

[*Translation*]

I thank you very much for your presence and for your testimony.

Mr. Daniel Therrien: Thank you very much.

[*English*]

The Chair: We will suspend quickly so we can switch out the panel.

Thank you.

● (1520)

_____(Pause)_____

● (1520)

The Chair: We will now resume for the second panel.

With us for the second panel, we have Professor Teresa Scassa, the Canada research chair in information law and policy at the University of Ottawa; and Mr. Michael Bryant from the Canadian Civil Liberties Association.

We will start with presentations for five minutes each, followed by rounds of questions.

I will just remind the witnesses that if they see the yellow card, that means they have 30 seconds remaining. The red card means that the time is up.

With that, I will turn the floor over to Professor Scassa.

You have five minutes, please.

Prof. Teresa Scassa (Canada Research Chair in Information Law and Policy, Faculty of Law, Common Law Section, University of Ottawa, As an Individual): Thank you, Madam Chair and committee members, for the opportunity to address this committee on privacy in Canada's COVID-19 response.

We're currently in a situation in which Canadians are very vulnerable economically, socially and in terms of their physical and mental health. Canadians know that sacrifices are necessary to address this crisis and have already made sacrifices of different magnitudes. Most Canadians accept that this is necessary to save lives and begin to return to normal. They accept that some degree of privacy may need to be sacrificed in some contexts, but there is no binary choice between privacy and no privacy. Instead, there must be a careful balancing of privacy with other public interests.

There are two overarching privacy concerns when it comes to Canada's response to the pandemic. The first is that there's a risk that poorly thought-out collection, use or disclosure of personal information will create privacy and security vulnerabilities with little real benefit, or with benefits disproportionate to risks and harms. The second is that the pandemic may lead to the introduction of data gathering or processing technologies that will create a new normal, leading to even greater inroads on privacy, dignity and autonomy. Importantly, surveillance often has the most significant adverse impacts on the most vulnerable in our society.

The pandemic context raises a broad range of privacy issues, from government or law enforcement access to location and personal health information to contact-tracing apps and beyond. As we begin the return to normal, we will also see issues of workplace surveillance as well as tracking tools and technologies used to help determine who gets into stores, who receives services or who gets on airplanes. Personal health information, generally considered to be among our most sensitive information, may become a currency we're required to use in order to carry out ordinary daily activities.

Since time is limited, I'd like to tease out three main themes. The first theme is trust. Trust is referenced in the digital charter and is essential when asking Canadians to share personal information with the government, but trust is complicated by a pandemic context in which issues evolve rapidly and are often unprecedented. One thing that trust requires is transparency, and governments have struggled with transparency, whether it's with respect to sharing data that models the spread of COVID-19 with the public or, as was the case with Alberta, launching a contact-tracing app without releasing a privacy impact assessment. Transparency is essential to trust.

The second theme is necessity and proportionality. The Privacy Commissioner of Canada, along with his provincial and territorial counterparts, supports an approach to privacy based on necessity and proportionality. This is derived from the human rights context. Necessity and proportionality provide a robust analytical framework for balancing privacy rights against other public interests and should already be part of an amended Privacy Act.

The importance of this approach cannot be overemphasized. We are in a data-driven society. It's easy to become enthused about technological solutions, and innovators promise that data analytics, including AI, can solve many of our problems. We need to remember that while technology can provide astonishing benefits, there is already a long history of poorly designed, poorly implemented and often rushed technological solutions that have created significant risks and harms. Novel technological solutions often fail. This is becoming a reality, for example, with many recently launched national contact-tracing apps. Rushed, flawed schemes to harvest personal data, even if for laudable goals, will erode trust at best and cause harm at worst. This is why clear guidelines, such as those developed by the commissioners, are crucial. There should be an emphasis on purpose and time-limited solutions that minimize privacy impacts.

The third theme is human rights. Privacy is closely tied to human rights, but this relationship is increasingly complex in a data-driven society. Privacy laws govern data collection, use and disclosure, and it's increasingly common for data uses to have significant impacts on human rights and civil liberties, including freedom of association, freedom of speech and the right to be free from discrimination.

Until recently, public conversations about contact tracing have been predominantly about government-adopted apps to deal with public health and disease tracking. As businesses reopen and people go back to work, the conversation will shift to contact tracing and disease monitoring in the private sector, including the possible use of so-called immunity passports. We will see workplace surveillance technologies, as well as technologies that might be used to limit who can enter retail stores, who can access services, who can get on airplanes and so on.

While there are obviously serious public health and safety issues here, as well as issues important to economic recovery and the ability of people to return to work, there is also significant potential for harm, abuse and injustice. Much of this private sector surveillance will be in areas under provincial jurisdiction, but by no means all of it. The federal government must play a leadership role in setting standards and imposing limitations.

I'll end my remarks here. I look forward to your questions.

● (1525)

The Chair: Thank you very much, Professor Scassa.

Our next presentation is by Mr. Bryant. You have the floor for five minutes.

[*Translation*]

Hon. Michael Bryant (Executive Director and General Counsel, Canadian Civil Liberties Association): Good morning, Madam Chair; thank you very much.

Thank you all for being here this afternoon.

[*English*]

You will be glad to hear that that's the end of my French. My kids will be glad to hear it anyway. They're bilingual and obviously I'm not.

I've provided some speaking notes, which I hope all the committee members have. If they don't, I'll send another copy to the clerk.

It's a letter that I and Brenda McPhail of the Canadian Civil Liberties Association wrote to the Prime Minister and first ministers on April 20. We've set out a set of principles that would apply not to private sector apps per se or private sector technology and contact tracing per se, but to any requirement under provincial or federal law that would mandate the use of some technology. Hopefully that may be a very narrow category, but that's where, as lawmakers, we feel there's a process and some principles that apply. We may discuss them, but it's listed there in that letter. It's a set of nine principles.

I want to start with jurisdiction and make a pitch for there being a national perspective on this. The point of Confederation in 1867 was that we would be able to do more together than we could apart. That is being tested during this emergency management for federalist reasons. I think, rightly, the provinces and territories are playing the role they ought to play; however, there is a role for parliamentarians. Exactly what that role is, other than the economic relief that is being promised, is something this committee ought to address. I believe that having some basic human rights standards and some very basic goals for technology-assisted efforts to tackle COVID would be an appropriate role for parliamentarians to play.

A practical consideration, and one that I think is going to end up being the sad truth—I wish it weren't so—is that I don't think these systems are going to work, in 2020 anyway. I think there's a very real chance that the technological systems we're talking about today will simply not prove practical in real-world conditions. Their accuracy rate may be just too low and the complexity of human interactions just too high, because it renders too many false alarms.

Second, I think it's very vital that we be able to take a step back and recognize that a contract-tracing application on its own does nothing to stem the spread of COVID. It's useful only if those who learn of a possible exposure to COVID are able to do something about it: get tested, get counselling, get treatment or take measures like self-isolation. But if those services aren't available, if that testing isn't available, if it's not possible for somebody to self-quarantine without going into bankruptcy, then these technological ideas are useless. The advice that encourages self-isolation isn't plausible if at a certain point people can't do it, and they won't do it, as was suggested previously.

Furthermore, the thinking through of what proportionality looks like after necessity is established is important. Proportionality means looking at other, less intrusive means of getting at what you're trying to get at. To start out with mandatory adoption of a contact-tracing app, with a serious fine attached to failure to download the app, would never be proportionate in 2020, because the efforts of undertaking this exercise with less intrusive means have to be established first.

● (1530)

Finally, the United Kingdom released their app just this week. They weren't prepared properly and it was a disaster. It was a complete disaster and an embarrassment to the country. I would encourage us to get everything lined up first, and the protections lined up first, before the app starts.

Thank you.

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

We'll now go to our round of questions.

MP Gray, you have the floor for six minutes.

Mrs. Tracy Gray (Kelowna—Lake Country, CPC): Great.

Thank you very much, Mr. Bryant, for your testimony today.

Last week, we had Google Canada here at this committee. As you may know, they're releasing those community mobility reports, which track people's movements from their homes to places like parks and transit. They track users' locations from their phones. Google Canada stated that their data is aggregated and anonymized to protect users' privacy, but some data reidentification experts state that location data can never truly be anonymized.

Mr. Bryant, would you agree with that assessment?

Hon. Michael Bryant: Yes, on the latter assessment, I would. We have expert reports that we filed in the court before Google decided to exit their sibling corporation, and at CCLA we're in litigation over the Quayside project. We filed a number of expert reports. It's on our website, CCLA.org. We make the case that, in essence, anonymizing or de-identification is an overstatement. That's not what happens.

In fact, reidentifying, depending on the particular program, is anywhere from self-evident to easy. Certainly, I think using the term “anonymizing” or “de-identifying” in itself is misleading.

● (1535)

Mrs. Tracy Gray: Thank you for that. That is certainly concerning.

Mr. Bryant, Google Canada also stated that they did not notify their users that they would be using their data in these mobility reports. Do you think Google Canada should have done so?

Hon. Michael Bryant: Yes. I think people deserve to be able to consent, to opt in, and at the very least to be able to opt out. The main reason this is happening in Canada is that Canada does not have the equivalent of the EU GDPR. Canada does not have the equivalent of the California privacy law, for example.

The failure of this government to get a modern data privacy regime in place, in however many years they've been in office, is an enormous failure. It took about 10 years for the EU GDPR to get developed and worked out before it was released and done. As far as I can tell, although this committee would know better than anyone, federally we're not where we ought to be. That type of law wouldn't work in the EU. Google couldn't do what they're doing in Canada.

Mrs. Tracy Gray: I know that the Canadian Civil Liberties Association discusses the idea of “meaningful consent” when it comes to such things as contact-tracing apps. Do you think Canada's current privacy laws are adequate enough for these companies, using location data from their users, to meet the threshold of meaningful consent?

Hon. Michael Bryant: No.

Mrs. Tracy Gray: Well, that says it right there.

I guess that leads to my next question, which has to do with the government considering putting in place contact-tracing apps during this pandemic. Some cybersecurity experts are stating that to put these tracing apps in place, Canada would need new legislation to set boundaries and protect Canada's privacy. Would you agree with this?

Hon. Michael Bryant: I generally advise against legislating on the subject of emergency management during an emergency. The uncertainty and fear that are present at the time of a pandemic interfere with and disproportionately adversely affect individual rights. In essence, everything ends up being like the U.S. Patriot Act.

Under those circumstances, I'm nervous, I should say, about legislating at this time, because I don't think adequate protection for human rights would be found. Be that as it may, there nevertheless can be a lot put into place, apparently, by way of emergency management cabinet orders in council, provincially and federally. The powers exist to put those protections in place.

I'm ducking that question a bit, because I'd rather our privacy laws not be legislated right now in Canada. At the end of it, I think it would be a mistake, and it would be bad news for civil liberties.

Mrs. Tracy Gray: Madam Chair, do we have time for one more question? I think we're going up against the clock here.

The Chair: You have 45 seconds.

Mrs. Tracy Gray: As one last quick question, then, do you think Canada's current privacy laws are sufficient to protect Canadians' data on potentially widely used apps that will track their location and personal data for contact-tracing purposes?

Hon. Michael Bryant: No, I don't, but that doesn't mean that something couldn't be put together that provides some temporary protections. I think that's a job for parliamentarians to tackle so that we don't have one set of rights in Alberta, another set of rights in Newfoundland and another in Ontario. This would be an area where we ought to have a national standard and aspire towards that, one that's superior to those jurisdictions that have little respect for human rights.

The Chair: Thank you very much.

Our next round of questions goes to MP Lambropoulos.

You have the floor for six minutes.

● (1540)

Ms. Emmanuella Lambropoulos (Saint-Laurent, Lib.): Thank you, Madam Chair.

Thank you to all our witnesses for being with us today.

My first questions are going to go to Professor Scassa.

Federal privacy laws really have not been substantially amended since their enactment. The Privacy Commissioner of Canada noted, in a joint statement with his provincial and territorial counterparts, that our current laws do not provide an appropriate level of protection to Canadians with regard to their privacy, given the digital environment. He actually mentioned it again today during the first panel in this meeting.

Do you agree with the joint statement and the principles it contains?

Prof. Teresa Scassa: Yes, I do. These are laws that were drafted at a time when we collected far less data and did far fewer things with data. They were written for a very different type of environment.

We are in a data-driven society. We need laws that are adapted to it.

Ms. Emmanuella Lambropoulos: Absolutely.

What changes to federal privacy laws do you think would be beneficial during this crisis or going forward in a future that is increasingly a digital environment?

Prof. Teresa Scassa: One thing that has been raised by so many critics of PIPEDA is enforcement: that there simply aren't enough teeth in PIPEDA, that there is inadequate enforcement of privacy rights. Therefore, that is one very important area that would have to be looked at.

Ms. Emmanuella Lambropoulos: Thank you.

Do you think COVID-19 has shed light on other gaps that we currently have with regard to our privacy laws?

Prof. Teresa Scassa: COVID-19 is a wake-up call in many respects. Essentially, it has caught us with our privacy pants down. We need to have the digital legal infrastructure in place so that we can respond to situations as they come up. We find ourselves in this situation with outdated privacy laws for the public and private sectors, and this is a disadvantage.

Ms. Emmanuella Lambropoulos: Thank you very much.

Since today we're really here to talk about a contact-tracing app that is potentially being developed, what are your thoughts specifically with regard to this contact-tracing app? Where do we draw the line between protecting the privacy of Canadians and the greater good of Canada's public health?

Prof. Teresa Scassa: That's an interesting question, because no two contact-tracing apps are created equal.

There are contact-tracing apps that focus on collecting only data about proximity of devices. There are contact-tracing apps that also collect GPS data, which could be useful to public health authorities in determining where there are outbreaks. As well, there are contact-tracing apps that are going to ask users to input symptoms and so on, and may use AI to provide analytics to supplement the lack of testing that we have. This is a very broad range of data collection. They are very different apps with different goals, and I think talking about contact-tracing apps in the abstract is really problematic and very challenging for Canadians.

I've seen surveys asking Canadians if they are in favour of or opposed to contact-tracing apps, but nobody knows what we're talking about. This is part of the issue of transparency. We have to be very clear about what our goals are, what kind of information we're planning to collect to serve what purposes, before people can really meaningfully engage with whether this is a good thing and something that people want to participate in.

Ms. Emmanuella Lambropoulos: Do you think at any point it is okay for these apps to be mandatory and not opt-in, and what is that point?

Prof. Teresa Scassa: There are two things. One is, for a general national contact-tracing app, we've already heard about the challenges with making that mandatory. There are serious civil liberty issues with forcing people to carry their cellphones everywhere and have them running these apps in the background.

The new wave that I alluded to in my comments, and it's coming very fast, is going to be mandatory contact-tracing apps in workplaces. People will be going back to workplaces where the employer says, “You must use this contact-tracing app if you want to be part of this workplace.” That may be necessary to prevent major outbreaks of disease or control them within workplaces, and we've certainly seen this as an issue, but those apps are likely to be mandatory.

In addition to these debates about the national contact-tracing app, we need to start thinking about what the boundaries and parameters should be for these mandatory workplace apps that are coming.

Ms. Emmanuella Lambropoulos: I know that Mr. Bryant actually pointed this out earlier, or gave his opinion on this earlier. Do you think this type of app, or any contact-tracing app, is an effective way of making sure that we don't spread this type of virus, specifically given the qualities of COVID-19 and its symptoms and the way people can carry and spread the virus?

● (1545)

Prof. Teresa Scassa: Effectiveness really depends on what the goals are. If the goals are to replace human contact tracing, I don't think it will be effective. If the goals are to support or supplement it, depending on the design, possibly there will be some usefulness there.

If the goals are to actually collect, indirectly, data that can be used in analytics for disease modelling, then maybe there will be some useful data collected, but that's a different message that needs to be sent to Canadians.

I think that understanding what it is we're talking about and what the goals are for using such an app is really important.

Ms. Emmanuella Lambropoulos: Okay.

I saw the yellow flag, so I imagine I have less than 20 seconds left.

Thank you very much for your time.

[*Translation*]

The Chair: Thank you very much.

The member for Abitibi-Témiscamingue will be the first speaker in the next round.

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

Mr. Sébastien Lemire: Thank you, Madam Chair.

My first question is for Ms. Scassa.

I think the most important question to answer is, who does the data belong to?

Should the data of a COVID-19 positive case belong to the individual, since it is his or her medical record and he or she has a right to privacy, or should it belong to the state, in order to limit the spread of the pandemic?

[*English*]

Prof. Teresa Scassa: The question of ownership of data, the language of ownership, can be a bit problematic or misleading in this context. In the Canadian approach, we've always talked about interests in data. We recognize that there can be multiple interests in data. A private sector company that collects data has an interest in the data they collect. The individual they collect it from has an interest in that data, and there may be other interests.

It's the same with personal health information. The health system has an interest in data collected through the medical system, for a variety of purposes, and the individual has an interest in that data.

The GDPR is a model that pushes us much more towards.... Well, it strengthens those interests. It doesn't assign ownership of data either, but it does provide for stronger interests on the part of the individual. Right now, I think we're in a data protection framework, particularly at the private sector level, that gives individuals considerably less interest in or control of their data than you would see in the European context.

I think that in all cases it's really a matter of interests, and you can have multiple interests in the same data.

[*Translation*]

Mr. Sébastien Lemire: Mr. Bryant, in your opinion, should the data relating to a positive COVID-19 case belong to the medical file, and therefore to the individual, or should it belong to the state in order to limit the spread of the virus?

[*English*]

Hon. Michael Bryant: It would belong to the person, and I would argue against it belonging to the state at this time. There's no evidence to suggest that once having that information.... I should say at the outset that I agree with everything Professor Scassa said and will say, and you can hold me to that.

First, the discussion about this turns in part on centralized systems versus decentralized systems. Germany started out arguing for a centralized system and ended up arguing for a decentralized system that gave people control over their information. I think that information about a person belongs to that person; it doesn't belong to the state. The state may have some interest in it, as the professor said, but we need to start with trusting people.

Second, the state may play a role in incentivizing people to share that information. However, only once every other mean has been exhausted should the state ever consider trying to take ownership over that information.

We talk a lot about what is mandatory and not mandatory in Canada. It's extraordinary to me that this country has come to that. Very little about the incentivizing that can take place can get even greater compliance. This is compliance with the use of the contact-tracing apps, compliance with respect to reporting and compliance with respect to self-quarantining. Sure, I guess you could use a stick to try to get people to do it, but I would argue it's going to be ineffective. People won't use it; it will be avoided. The alternative is to provide incentives for that.

In the United States, an economist at The University of Chicago talks about how much money would be saved if governments paid people to comply, to self-isolate and to get tested every week, for example, or created some incentive so that when people participate in it, they get some kind of a benefit. It might end up being a lottery, with, in essence, a pandemic lottery ticket. We're talking about the author of *Freakonomics*. I think it's safe to say that economists at The University of Chicago can be respected and taken seriously.

The idea is to try to internalize the externalities. We should be doing more of that in allowing people to take the information they own and use it in a way that aligns with what the state wants from them.

● (1550)

[*Translation*]

Mr. Sébastien Lemire: Thank you, Mr. Bryant.

That was indeed a complete answer. It shows me how much responsibility we as parliamentarians and legislators really have in this situation. It's not for private enterprise to make the decision for us.

I'll give the floor to Ms. Gaudreau for a question.

Ms. Marie-Hélène Gaudreau: My question is for Mr. Bryant. We know our laws are outdated; we ask companies where our data is and what they do with it.

We make everything anonymous, as Ms. Scassa mentioned, and we legislate specifically for one application. What do you think of that in the context of a pandemic, in the context of an emergency?

[*English*]

Hon. Michael Bryant: I don't want any of my previous comments to suggest that the work to be done on privacy legislation should not take place.

The Chair: Could you wrap up really quickly?

Hon. Michael Bryant: Yes.

Draft the laws. Start debating the laws. Make them public. Have a conversation with the public about them. But I would not take them to the legislature in the middle of a pandemic.

[*Translation*]

The Chair: Thank you very much.

[*English*]

Our next round of questions goes to MP Masse.

You have six minutes.

Mr. Brian Masse: Thank you, Madam Chair, and again, thank you to the witnesses. My question will be for both witnesses.

I represent Windsor, Ontario, and it's right across from Detroit, Michigan, where there's a significant outbreak—amongst the highest in the world, really. In regular times, when we have international movement.... I'll use the river that separates us as an example, and the fish. You can tell the fish they're supposed to be on the American side or the Canadian side, but they don't listen; they'll go back and forth.

What I see happening with some of the discussions taking place with contact and data tracing is that we have a global pandemic, yet we have many pockets of contact tracing going on, with an attempt to protect personal privacy, as well as ensure confidence in the management of the system and so forth.

I'm just wondering if you have any comments about the value of it, given the fact that it is a global pandemic. We have people in our own country, now as it is, with multiple platforms on their cell and mobile information-sharing devices; and then potentially we have other factors of foreign visitation, even during the worst of times, that are still happening.

We also have essential workers travelling back and forth. Normally, in Windsor here there are 10,000 trucks a day and 30,000 vehicles. It's down significantly, but it's still in the thousands of vehicles.

I'm just curious as to the data that we'll get from this and given the fact that it seems to be compartmentalized amongst different countries.

Maybe, Mr. Bryant, you could go first.

Hon. Michael Bryant: Thank you.

I confess that I'm not sure I understood your question, but I'm going to take my best shot at addressing it.

I would agree, if I understand you correctly, that there are just so many different ways in which the virus is being fed, many of which we don't even know, and some of which, yes, continue to arise from people from other jurisdictions, and much of it, as you mentioned, being found in larger urban centres. For example, in Ontario it's more so that Windsor, Toronto, London and Ottawa continue to have a pandemic crisis, and in much of the rest of the province, there's really not so much.

In that sense, the context in which contact tracing, for example, would be useful and helpful may be quite limited in urban centres—extremely limited—and at this stage possibly useless. That's not to say that down the line it would not be useful in those regions where there's a very small population, and that's a way in which to keep the virus from spreading at all.

The way in which this virus is going to be reduced by way of contact-tracing apps in urban centres.... There may be a correlation, but I don't know if we'll be able to say, oh, this caused that. On the other hand, in smaller populations it may be otherwise.

I'm going to let the professor take it from here.

● (1555)

Prof. Teresa Scassa: Thank you.

I was just reading about how Northern Ireland, which is part of the U.K., has declined to implement the U.K. contact-tracing app in favour of adopting a solution that's compatible with the Republic of Ireland, with which they share an island, because that's their choice. They're thinking in terms of where their people are travelling and where their people are moving.

I think we started off small for a while. Ottawa Public Health was talking about adopting a contact-tracing app at a time when nobody was leaving Ottawa, we were all staying home, and that's where we needed an app. But now we're going to start opening things up and we need an Ontario app.

When Alberta adopted its app, the push-back, which I think you are feeling right now as parliamentarians, was that we needed a national solution, because as soon as we start opening things up people are going to be travelling across the country. If you don't have something that works across borders, then it's not going to be particularly useful, especially, of course, here in Ottawa where we share a border with Quebec and people travel back and forth all the time.

I think as our circumstances change so does the vision of what we have to deal with, which has an impact on what technology we adopt. This is all moving so quickly that I think it's been hard to adapt and respond to it. Again, I'm going to make a plug for thinking about the next thing, which is workplace employment contact tracing. I think this is the big wave that's coming and I think it's going to be a really important one.

Mr. Brian Masse: That's actually really good.

I only have a few seconds, so really quickly, with that, would it make sense, then, if we are going down this road, to almost, again, have it like a specific bond or agreement between the employer and the person, and in the second event, between the country and the person, or is it just an overall country policy?

I'll leave it at that, because there's no time.

Prof. Teresa Scassa: Perhaps I can respond very quickly. With workplaces, I think we're going to have to be looking at PIPEDA, and we're going to be looking at provincial laws to the extent that they're applicable in Alberta, B.C. or Quebec. That's where we're going to have to look for solutions, and I don't think there are particularly good ones right now.

The Chair: Thank you very much.

Our next round of questions goes to MP Patzer.

You have the floor for five minutes.

Mr. Jeremy Patzer: Thank you, Madam Chair.

My first question is going to be for Mr. Bryant. I'm just looking for a simple yes or no.

Is data ownership considered private property?

Hon. Michael Bryant: Is my data my property? I would say yes, that's my property, but I have a qualification. I know you wanted a yes or no, but you get to ask the questions and I get to give the answer.

Mr. Jeremy Patzer: That's fine. If you want to give that qualification, just do it quickly, if you wouldn't mind.

Hon. Michael Bryant: I'd just repeat what the professor said about other actors, including having an interest in it, and choices need to be made about who gets that interest.

Police would probably like my private data, because police like that kind of information; it assists their investigations. However, you would want to forbid data leakage outside of the public health context.

Mr. Jeremy Patzer: Right. The reason I asked is because I'm just concerned that, in the Constitution, private property isn't really a constitutionally protected element.

Anyway, I'm going to move on to my next points here.

There were already concerns about the freedom of the press in the last couple of years, prior to the pandemic. Unfortunately, with Parliament suspended and its powers limited, there is much more of a need for the media to openly follow and question the government's decisions and activities.

Are there any barriers or concerning trends for Canadian media to access or challenge the government, especially since lockdowns began?

● (1600)

Hon. Michael Bryant: There's no question that there's an absence of accountability.

For example, I'm concerned that when there are announcements made by government ministers—we'll just talk about the federal government—when announcements or daily updates are provided, how much of that has legal authority, versus how much of it is just the person's opinion?

What would be helpful in these daily updates is, “The cabinet has passed the following orders in council. Here is what they are. Here is where you go find them on a website. Now let me tell you my personal opinion about things that have no legal authority.”

Because we don't know what is law and what is not, the rule of law is thrown into question, accountability is certainly thrown into question, and democracy is not aided by all that. That would be what comes most urgently to mind that threatens accountability of the executive to the legislature. The extent to which the legislative members feel shut out by that is something that I guess is for the members to decide how to remedy.

Mr. Jeremy Patzer: Yes. Well, thank you for that.

In recent months, we have seen the federal government play with the idea of shutting down what they consider fake news being spread online regarding COVID-19. However, a few months ago, it seems the government spread some fake news itself regarding masks, human transmission of the virus and the origins of the virus. It was all inaccurate.

How damaging would these measures be to Canadians' freedom of speech, but also for the freedom of the press?

Hon. Michael Bryant: We would argue against any measure by any government or any legislature seeking to in any way chill, let alone censor, people in terms of their freedom of expression.

Mr. Jeremy Patzer: What are the unintended negative consequences that such measures could create?

Hon. Michael Bryant: Well, who has a monopoly over the truth? Are we willing to say that the government or a legislature has a monopoly over the truth? No, of course not.

If we can agree that governments don't get to decide what's true or not true, then they can't get the power to decide what information ought to be circulated to others.

Mr. Jeremy Patzer: This next question I would like you, Mr. Bryant, to answer first, then Professor Scassa, perhaps you wouldn't mind answering as well.

Last week we heard a witness from a private company describe their work with provincial health databases as creating, and I quote, “a single source of truth”.

Do you have any concerns about how governments and companies are planning to collect and manage data?

Hon. Michael Bryant: Yes.

I think I'm going to let Professor Scassa go first since I took all the last few questions.

Prof. Teresa Scassa: Yes, I always have concerns about how data collection and use is going to take place, especially as we move into a time of big data analytics and artificial intelligence, because the uses can go beyond what we've even imagined before. I do think we need to have strong privacy legislation in place and strong accountability and oversight.

Mr. Jeremy Patzer: Thank you.

The Chair: Our next round of questions goes MP Ehsassi. You have the floor for five minutes.

Mr. Ali Ehsassi (Willowdale, Lib.): Thank you, Madam Chair. Thank you to the witnesses for appearing before our committee today.

As you both may have heard, we've just heard that the only province that has actually launched a tracing app, Alberta, is still waiting to hear from its privacy commissioner as to whether that app actually lives up to the standards that were set out in the joint statement released on May 7. I just took a look at the website of the Alberta privacy commissioner and it says that privacy impact assessments can take up to a year.

I'm astounded because if we take the joint statement that was released by the provincial and federal privacy commissioners, did they mean to just provide us with some yardsticks, recognizing full well that it would take many months before a government could go there and ensure that all those safeguards are there?

What is the process that you would recommend a government adhere to?

Perhaps I could start off with Professor Scassa.

● (1605)

Prof. Teresa Scassa: My understanding is that there was already a privacy impact assessment that was carried out on the Alberta app. That's what the privacy commissioner of Alberta is reviewing. She is, I think, having discussions with the Alberta government. I think that's why we haven't yet had a verdict. She has some concerns that she wants to raise based on the PIA.

The Australian app that was released at the same time as their privacy impact assessment is quite a long, comprehensive document that they posted on their website as well.

It is possible to have a privacy impact assessment done quickly. The Australian PIA, for example, flagged some serious issues which the legislature in the Parliament in Australia is now considering and taking into account and looking at legislation.

Where there is a need and a sense of urgency, things can move more quickly. I know that the privacy commissioner talked about talking with Mila about their app and providing advice and consultations with Mila. There are ways for things to happen quickly. Not everything is going to be on slow time.

I have confidence that this work can be done and can be done quickly to improve privacy with these types of apps, even in a crisis.

Mr. Ali Ehsassi: Mr. Bryant, would you like to add anything to that?

Hon. Michael Bryant: Yes.

I think there's a difference between a final assessment on the one hand and getting some feedback from a privacy commissioner on the other hand. I know the federal Privacy Commissioner would welcome an opportunity to appear before this committee or appear before anybody who asked them to, to come in and provide a preliminary set of opinions. Where a privacy commissioner says, “Look, I just need some more information”, they can provide that information. But more often than not they are able to say, “Look, if this, then that”, and so on.

I think that answer was, in part, typical of that privacy commissioner. Secondly, it was also driven by the fact that if you're seeking a final answer, they're not going to have one for a while. That doesn't mean we can't get preliminary answers.

Mr. Ali Ehsassi: Thank you for that.

Now perhaps I could return to Professor Scassa.

In your opening remarks you flagged the issue of workplace privacy. That is actually one of those issues that we very seldom hear about in the papers. Could you elaborate on that? What are the things we should be very much concerned about?

Prof. Teresa Scassa: My understanding is that there are discussions taking place in Canada and in other countries, especially where there is a large workforce, about how people will be able to return to the workplace and be safe.

In that context, they are designing, developing and looking to implement contact-tracing apps within the workplace. They will basically monitor where people are within the workplace, who they interact with, where they move about and what their patterns of movement are within the workplace, so that if there is an outbreak of COVID-19 or if an employee is diagnosed with COVID-19, other employees can be notified and appropriate measures can be taken.

On the one hand, you can understand how important that is for getting people back to work and keeping them safe, but at the same time, that's a very significant level of surveillance. I think it raises privacy issues that we need to be thinking very seriously about when we put protections and balancing factors in place.

Mr. Ali Ehsassi: Mr. Bryant, did you want to respond? Actually, I'm out of time.

Thank you.

The Chair: Sorry, MP Ehsassi.

Our next round of questions goes to MP Rempel Garner.

You have the floor for five minutes.

Hon. Michelle Rempel Garner: Thank you, Madame Chair.

My first question is for Mr. Bryant.

You raised the GDPR and the CCPA earlier, which I think are two very important pieces of global best practice with regard to data. Article 20 of the GDPR speaks to the right of data portability, and the CCPA allows people to request that their data be deleted or to opt out of the selling of their data.

With that being best practice, would it be beneficial to Canadians to have that type of a data ownership regime, for lack of a better term, ported into law in Canada?

● (1610)

Hon. Michael Bryant: Yes, I do.

Hon. Michelle Rempel Garner: Thank you so much.

Just to build off the questions from my colleague Mr. Patzer and Mr. Lemire, what do you think of enshrining a right or an acknowledgement of personal data ownership? Right now there is a perception that due to onerous terms of service, data, or the productive value of data, is owned by, let's say, big data corporations. If we enshrined the right of personal data ownership as a principle or a starting point to build a new privacy framework in Canada, would that be helpful for Canadians?

Hon. Michael Bryant: I am not sure. The reason I'm not able to answer yes or no is that it depends on what's done with that information. If somebody can access the information that I supposedly own, that doesn't say much for my ownership rights.

The issue is more about presumptions. The presumption that it is private information should be the starting point, and then it's up to third parties and the state to make the case for access to that information.

That's the best way I can answer the question.

Hon. Michelle Rempel Garner: Thank you. That's very helpful.

Mr. Bryant, I've been a parliamentarian for several years now, and it's a learning experience. I've been on both sides of the aisle. What I've noticed in my tenure is that over this period there has been a big centralization of power within the PMO. I question the rights and abilities of parliamentarians under current operating situations, and what has happened in the last several months really concerns me as a parliamentarian and as one who represents over 80,000 electors. I want your thoughts on that.

For example, there are a couple of headlines that really disturbed me. One was in The Globe and Mail: “Health Minister Hajdu stops Dr. Theresa Tam from answering question about Canada’s emergency stockpile”. Also, my understanding is that the federal estimates, which are going to have about $150 billion of new spending, will only have four hours of debate. One of the things your organization does is it protects the right to vote. I have a right to vote on behalf of many of my constituents.

Are you concerned about the state of democracy and civil liberties with regard to how Parliament has been operating throughout this crisis? What are your recommendations to us on that?

Hon. Michael Bryant: I'll just repeat what I said before about accountability. There should be some clarity and transparency with respect to what the government is doing when it's considering a particular order, what the timeline is for an executive order and what the executive is doing at any given time. When a decision has been made by cabinet, it should release it immediately and be explicit about this, not putting it in the can, getting the communications ready and then making it available to the public. The—

Hon. Michelle Rempel Garner: I just have a few seconds left.

It's my understanding that the government has used an order in council to put forward a confiscation regime for property of law-abiding Canadians. Do you think that's acceptable during a pandemic?

Hon. Michael Bryant: I'd need to know more specifics about it, but I'd say it has to be authorized by legislation. If it's not authorized by legislation, it would be without jurisdiction.

Hon. Michelle Rempel Garner: Thank you.

The Chair: Our next round of questions goes to MP Erskine-Smith.

You have the floor for five minutes.

Mr. Nathaniel Erskine-Smith: Thanks very much.

Professor Scassa, I normally agree with everything you say. In this case, I agree with almost everything you say. I have one challenge. I'm probably speaking into a bit of a void here, because I don't think we're going to get to a place where these applications are as effective as they maybe could be, but one challenge getting in the way of that is the idea of requiring opt-in systems.

You are absolutely right that there are very different tracing applications. We can look to a decentralized system like the DP-3T standard, say, or look to using Bluetooth, which is more accurate than using GPS data. If we have a data governance framework in place that respects every principle on purpose limitation, that ensures that information will be deleted at the end of this pandemic and that has strong oversight from privacy commissioners or privacy advocates like you, and if it is true—and this may not be true, though there is some research out of Oxford that it is—that an adoption rate of 60% or higher is required for this to really have an impact and be successful, and we could save lives as a result, why is an opt-out system so important? Is it not a balance? Are we drawing the lines even before we get to the important question of what is effective overall and where the balance should be struck? Are we just saying, right from the get-go, that we can't even have this conversation because it should be opt-in?

● (1615)

Prof. Teresa Scassa: I think that's a really interesting question to unpack. I have trouble separating my own skepticism about the technology from the issue of whether it should be mandatory. For example, a lot of these technologies, depending on the design and depending on which one it is, depend on the effectiveness of COVID-19 testing. If you're in a context where not everybody's being tested and it takes five days to get test results, then these apps are going to be minimally effective. They may be useful in some circumstances.

Mr. Nathaniel Erskine-Smith: I agree with that, so let's imagine a world where we ramp up testing capacity to such a degree that there is a role for them to play. If there is a role for them to play, and adoption rates of 20% are, as we know, not going to be significantly effective and it's not even worth going down that road, let's double down on human resources. We should do that anyway, I agree, but if we can get to a 60% or 70% threshold by having an opt-out system that still preserves the choice of an individual who truly cares, wouldn't that make more sense, all else being true? I recognize that there are a lot of contingencies here about the data governance framework and the design of the tracing application, but if everything else preserves privacy in every way, is there any give on that particular issue?

Prof. Teresa Scassa: I think it's hard because in a sense you almost create a context that is not the realistic context we live in. You have people who don't have phones. You have people who don't have phones that are of the right model or operating system. You have people with perceptual disabilities. Some Canadians may have difficulty with the English- or French-language literacy levels necessary to use the apps. A number of people are going to be excluded, in any event, so I think in that context, mandatory or obligatory is problematic.

The other issue is the civil liberties issue of making a form of data collection about location, context and personal health information mandatory. I think once you set a precedent for saying mandatory—

Mr. Nathaniel Erskine-Smith: No, I've suggested opt-out, right?

Prof. Teresa Scassa: You're saying opt-out, yes.

Mr. Nathaniel Erskine-Smith: That's different from mandatory.

Prof. Teresa Scassa: Yes.

Mr. Nathaniel Erskine-Smith: It still preserves choice in a significant way. I think it would strike a better balance overall, but it requires a lot of other contingencies to be put into place.

Prof. Teresa Scassa: It does, yes.

Mr. Nathaniel Erskine-Smith: Mr. Bryant, you were speaking to the importance of freedom of speech. Of course, truth is important too. When it comes to social media companies, which are private actors that certainly have every right to downgrade content that is inaccurate and false and to highlight reliable sources, would you take any issue with broadcasting standards councils and other things like that, which would focus on and support truth and standards in the dissemination of information?

Hon. Michael Bryant: I'm all for truth, if that's what you're asking. Our concern is primarily with censorship.

Mr. Nathaniel Erskine-Smith: I do note, of course, if you say something false and it harms another person's reputation, of course you are restricted in saying that. So we do have censorship in a significant way in all sorts of contexts. Would you be opposed to the idea of social media councils in terms of the ethics of the information they are effectively pushing forward, as algorithms are replacing editors?

Hon. Michael Bryant: I would need to know more about it. We're the CCLA, so we have the luxury of being able to be hardline on free speech, which you don't have pragmatically. I think I'd better leave it at that.

Mr. Nathaniel Erskine-Smith: Thanks very much.

The Chair: Thank you very much.

[*Translation*]

I now yield the floor to Mr. Savard-Tremblay, who has two and a half minutes at his disposal.

Mr. Simon-Pierre Savard-Tremblay: Thank you, Madam Chair.

Once again, I thank the witnesses for their statements.

I want to ask you the same question I asked the Privacy Commissioner of Canada, but from a different angle.

Couldn't the concept of ownership of data be specifically addressed in the legislation that might be passed? On the one hand, we should be able to decide what we agree to share. On the other hand, in the event of a violation of privacy or use of data against the will of the person concerned, could the notion of ownership trigger the application of severe measures, as is already the case in some European countries?

● (1620)

[*English*]

Hon. Michael Bryant: Professor, the only thing I'll say is this: I think the control over the data is a more important question than ownership of the data. I'm not saying that the ownership is irrelevant, but I think for the purposes of the topic at hand, the issue is really about control and not about ownership. That's all I have to say, other than repeating myself with respect to the different interests that are at stake. I think some bottom lines would need to be set, for example around data leakage to police and other investigation institutions or agencies. They should not be getting what amounts to public health data under any circumstances.

Professor, what do you say?

Prof. Teresa Scassa: I think control is the issue. Right now our privacy laws are weak in comparison to, for example, the GDPR, in terms of the rights of control they give to individuals. They are also weak in terms of the enforcement if there are breaches of those rights. The rights of control are tremendously important, and I think we have work to do there.

[*Translation*]

Mr. Simon-Pierre Savard-Tremblay: Am I to understand that, for you too, the question of ownership is secondary when compared to the question of control?

[*English*]

Prof. Teresa Scassa: I think ownership is misleading. It's misleading and it's a distraction because there are these multiple competing interests. A company or an organization, an entity, that has collected data has an interest in that data, as does the individual from whom it's collected. To start talking about ownership in that context is meaningful. It's about rights of control.

[*Translation*]

The Chair: Thank you very much.

[*English*]

Our last round of questions will go to MP Masse. You have two and a half minutes.

Mr. Brian Masse: Thank you.

I'll go to Professor Scassa first, and then to Mr. Bryant.

Professor, I proposed a digital bill of rights that would basically enshrine your physical rights to be almost the essence of your digital rights. Without getting into the details on that, is that something we should have as a divining principle, or at least a benchmark, that we could then actually have protected by the Privacy Commissioner or the Competition Bureau and other different public agencies that rule on whether or not our information is abused, misused, and then have it modernized to be protected in Canada, but also for international agreements? That's the concept. It's more robust than that, but the essence of it is that your physical rights are replicated in your digital rights.

Prof. Teresa Scassa: It's an interesting concept. I have to confess that it's not one that I've thought a lot about. I don't want to waste your two minutes hemming and hawing and thinking about it.

Mr. Brian Masse: That's okay; no worries.

Mr. Bryant, do you have any comments on that?

Hon. Michael Bryant: I think I'd better undertake to have CCLA review it and get back to you with a proper answer, rather than providing a bunch of qualifications in your two minutes.

Mr. Brian Masse: That's fair. We've been working on this.

My last quick question is for Professor Scassa to start and Mr. Bryant.

Do we need to have, at the end of the day, international treaties as well to deal with consistency of our data use and management as part of our trade negotiations?

Prof. Teresa Scassa: I think we're getting to a point where we need to have international standards, because we are constantly running up against, for example, very low thresholds for data protection, which are below our own, with respect to U.S. companies, and this causes enormous problems. How we will get a consensus internationally and whether it will put us above or below the level of protection that we currently have is anybody's guess, but we do need to have some sort of international privacy consensus.

Hon. Michael Bryant: I think first we need to have a national consensus and we need some national laws. We need to update the data laws. I'm sure you don't disagree with that, but I'm going to put an emphasis on that. The international treaties are out of my jurisdiction.

● (1625)

The Chair: Thank you very much. That is all the time we have for today.

I really want to thank everyone for their patience and flexibility in terms of extending the time we had today.

With that, I call this meeting adjourned.