HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 133 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, January 31, 2019

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Thursday, January 31, 2019

● (1530)

[*English*]

The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)): Welcome, everybody.

Per the notice of meeting this is meeting 133 of the Standing Committee on Access to Information, Privacy and Ethics. The study is on the privacy of digital government services.

Today we have with us somebody we've had several times before, Daniel Therrien, Privacy Commissioner of Canada. We also have Gregory Smolynec, deputy commissioner, policy and promotion sector, and Lara Ives, executive director, policy, research and parliamentary affairs directorate.

Before I go to Mr. Therrien, I want to go to Mr. Kent quickly.

Hon. Peter Kent (Thornhill, CPC): Thank you, Chair.

Colleagues, I hope I'll get unanimous consent on this. In light of yesterday's announcement by the Minister of Democratic Institutions of this new panel to screen advertising, messaging and reporting during the upcoming election, I'd like to suggest that we allocate at least one meeting to call representatives of some of the seven organizations that the minister said would be looking to screen acceptable reportage and advertising.

The Chair: Mr. Angus.

Mr. Charlie Angus (Timmins—James Bay, NDP): If I hear the suggestion correctly, I think it would be worth our while. As with all-party unanimous recommendations about protecting the electoral system, our committee brought forward recommendations. I think it's worth our having a view on this.

It seems to me that I'm looking at something that's probably much more fitted to a plan right now that deals with cybersecurity and cyber-threats, whereas what we've found in threats to elections are much more subtle. The manipulations might be harder to find.

It would be good to see if these representatives have looked at our work and we can question them on it. I would be very much in favour of that.

The Chair: Mr. Saini.

Mr. Raj Saini (Kitchener Centre, Lib.): I don't mind, but I'd prefer a formal motion so at least I can think about exactly what you want and which organizations they are.

Hon. Peter Kent: Sure.

Mr. Raj Saini: We would absolutely entertain it.

Hon. Peter Kent: It's not required. I've moved it now. Let's vote on it now. If you see fit to defeat it, then we'll do a formal vote.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Can you repeat the exact language?

Hon. Peter Kent: In light of the announcement made by the minister yesterday with regard to the special panel being created with representatives across—

The Chair: The security task force, I think it is.

Hon. Peter Kent: —the security task force, including Privy Council, CSIS—the seven organizations that were named.. We would invite them to find out exactly how they consider their new assignment, and perhaps give them a few weeks to get their heads around it. I assume they knew about it before the minister announced it yesterday, but it would be to have them talk about what they consider their mission to be, and how they'll carry it out.

The minister yesterday wasn't able to speak about where the red lines would be drawn in alerting Canadians to potential violation, or the intention of the panel, but I think it would be helpful, particularly given the work that we've done on this specifically for the past year.

The Chair: Is it Raj next and then Charlie?

Mr. Charlie Angus: I have language for a motion.

The Chair: Okay. Go ahead, Mr. Angus.

Mr. Charlie Angus: It's, “That the committee invite the appointed security task force of the seven organizations”—we could name them—“to brief the committee on their role in protecting the integrity of the Canadian electoral system for the 2019 election.”

The Chair: Just to be clear, are you providing words for Mr. Kent?

Mr. Charlie Angus: Yes. He was explaining what he wanted, but I think what we want very simply is a briefing from the appointed security task force on their role and plan for protecting the integrity of Canada's electoral system.

Hon. Peter Kent: Chair, I can give you the specific list now; the app has loaded: the Clerk of the Privy Council, the federal national security and intelligence adviser, the deputy minister of justice, the deputy minister of public safety, and the deputy minister of global affairs Canada. It's a pretty esteemed panel.

The Chair: Ms. Fortier.

● (1535)

Mrs. Mona Fortier (Ottawa—Vanier, Lib.): I would like to adjourn the debate on the motion and let the commissioner present.

The Chair: We're going to Mr. Therrien's testimony first, and then we'll come back to it after. Is that fine?

Hon. Peter Kent: The Liberals wish to seek guidance.

The Chair: Is that fair, Mr. Angus?

Mr. Charlie Angus: I just want to clarify the rules. Asking to adjourn debate, I don't believe it does. I would imagine that Peter would agree to defer it.

The Chair: We're going to vote.

Mr. Nathaniel Erskine-Smith: Assuming we're going to get back to the question....

The Chair: We're voting on adjourning the debate.

(Motion agreed to)

The Chair: I guess we'll get—

Hon. Peter Kent: As long as we vote by the end of the meeting....

The Chair: Okay. Sure.

Mr. Therrien, go ahead.

[*Translation*]

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

Members of the committee, thank you for inviting me to provide my views in the context of your study of the privacy implications and potential legal barriers relating to the implementation of digital government services in Canada.

A good starting point for this study, given that it defines the government's approach, is the government data strategy roadmap, published in November 2018, which was shared with us late last year.

In that document, the government indicates:

> Data have the power to enable the government to make better decisions, design better programs and deliver more effective services. But, for this to occur, we need to refresh our approach.
>
> Today, individual departments and agencies generate and hold a vast, diverse and ever-expanding array of data. These data are often collected in ways, based on informal principles and practices, that make it difficult to share with other departments or Canadians. Their use is inconsistent across the government and their value sub-optimized in the decision-making process and in day-to-day operations.

We of course support the use of technology to improve government decision-making and service-delivery but, as mentioned in your mandate, this must be done while protecting Canadians' privacy. In that regard, it is important to remember that privacy is a fundamental human right and that it is also a prior condition to the exercise of other fundamental rights, such as freedom, equality and democracy.

The government's roadmap underlines the difficulty of sharing data across departments and attributes this either to informal principles and practices or, in other circumstances, to legal barriers. I understand that there is in fact an exercise within government to identify these legal barriers with a view to potentially eliminating those found inconsistent with the new approach that the government feels is required to extract value from data.

I would say that what is a legal barrier to some may be seen as a privacy safeguard by others. The terminology that the government or other interveners use in this debate is not neutral. Many of the presumed barriers are found in sections 4 to 8 of the current Privacy Act. Should these rules be re-examined with an eye to improved government services in a digital age? Certainly. Should some of these rules be amended? Probably.

But, as you go about your study, I would ask you to remember that, while adjustments may be desirable, any new legislation designed to facilitate digital government services must respect privacy as a fundamental human right. I can elaborate on this point in the question period, if you wish. In other words, modalities may change but the foundation must be solid and must respect the rights to privacy. The foundation must be underpinned by a strengthened privacy law. As you know, we made recommendations to that effect in 2016. I would add a new recommendation here: that the public sector adopt the concept of protecting privacy from the design stage.

● (1540)

[*English*]

I reviewed with interest the testimony before you by officials from Estonia at the launch of your study. While the Estonian model is often discussed for its technological architecture, I was struck by the fact that officials emphasized the greater importance, in their view, of attitudinal factors, including the need to overcome silos in state administration leading to reuse of personal information for purposes other than those for which it was collected.

This could be seen as validation of the view that our Privacy Act needs to be re-examined and that—quote, unquote—"legal barriers" should be eliminated. I would note, however, that in Estonia the elimination of silos did not lead to a borderless, horizontal management of personal data across government. Rather, in the Estonian model, reuse, or what we would call sharing of information, appears to be based on legislation that sets conditions generally consistent with internationally recognized fair information practice principles and with the GDPR, although I would encourage you to follow up with Estonia as to what these legal conditions actually are.

As to the technological aspects of the Estonian model, our understanding is that there is an absence of a centralized database. Rather, access is granted through the ability to link individual servers through encrypted pathways with access or reuse permitted for specific lawful purposes. This purpose-specific access by government agencies likely reduces the risk of profiling.

We understand that further privacy and security safeguards are attained through encryption and the use of blockchain. This is in line with one of our recommendations for revisions of the Privacy Act in 2016, namely, to create a legal obligation for government institutions to safeguard personal information.

I note that the Estonian model is based in part on a strong role for their data protection authority, which includes an explicit proactive role as well as powers to issue binding orders, apply for commencement of criminal proceedings and impose fines where data is processed in an unlawful manner or for violations of the requirements for managing or securing data. Similarly, the OPC should have a strong oversight and proactive role in line with our Privacy Act reform recommendations.

I'd like to conclude with some questions for you to consider as you take a deeper dive into the Estonian model or discuss its applications in a Canadian context.

First, we've heard officials say that the success of the system is based on strong trust, which requires strong safeguards. But no system, as you know, is totally safe. What mitigation measures are in place in Estonia when, and not if, there is a breach?

Second, Canada's data strategy road map posits that one of the valued propositions of a model such as Estonia's is the intelligence to be gathered from data analytics, but it is unclear to us how, given the segregated set-up of the data sets and the legislative regime in which it operates, providing for specific reuse for specific purposes, this could be accomplished. You may wish to explore this issue further.

Finally, we would suggest that obtaining clarity from Estonian officials on the legal conditions for reuse of data would help, because that's an important safeguard to ensure there is no overall profiling and what I refer to as borderless, horizontal data sharing.

Thank you for your attention. I'll be glad to answer your questions.

The Chair: Thank you again, Mr. Therrien.

First up for seven minutes, we have a combination of Nate and David to start.

Go ahead.

Mr. Nathaniel Erskine-Smith: Thanks very much.

My first question is about the Estonian model and legal pathways.

When Michael Geist was before us, he said that technological measures put in place sound great, but we couldn't trust in those measures and we needed to revisit the Privacy Act. I take it you are of the same view.

Revisiting the Privacy Act and the clarity of pathways for sharing of information, I understand in Estonia, yes, they have a tell-us-once model, but you require specific statutory authorities for that reuse, so your point about our clarifying what the Estonian legislation says is important.

With respect to the Privacy Act, it's also your view, I suppose, that we should clarify the pathways of sharing information here in Canada as well.

Mr. Daniel Therrien: Yes. We have long-standing rules, of course, to govern the conditions under which data can be shared between departments. Those are essentially sections 4 to 8 of the current public sector Privacy Act.

Your mandate speaks to legal barriers. The federal government's data strategy road map talks about potential legal barriers. I assume that when the government refers to barriers, they are referring to revisiting or reviewing whether sections 4 to 8 are still fit for a purpose. I accept that, but I say at the same time that these are important rules, and although certain adjustments and modalities can be envisaged, let's not lose sight of the main principle, which is that privacy should be respected.

● (1545)

Mr. Nathaniel Erskine-Smith: Has the government come to you at all to discuss a digital ID project in any way?

Mr. Daniel Therrien: We had some discussions with government late last year about their data strategy road map, at a high level of generality, I would say. We were invited recently to offer views on strategies that individual departments are required or invited to adopt pursuant to the road map. That process has not started, but I welcome the invitation by government for us to give our advice.

Mr. Nathaniel Erskine-Smith: With respect to digital ID specifically, I understood that maybe there were some conversations under way at the federal level to pursue a digital ID project in concert with provinces. Have you been consulted on this specifically?

Mr. Daniel Therrien: This has been going on for a number of years. Perhaps Ms. Ives wants to add to this.

Ms. Lara Ives (Executive Director, Policy, Research and Parliamentary Affairs Directorate, Office of the Privacy Commissioner of Canada): Yes. I'll just add that there have been various iterations over the years. I think the most recent was in 2012. We reviewed privacy impact assessments for authentication rather than a digital ID: means to access online government services. One of them is issued by the Government of Canada and the other one utilizes banking credentials, but it's not exactly on point with the digital ID.

Mr. Nathaniel Erskine-Smith: I have a last question and then I'll turn it over to David.

Simply, are there examples of this government or previous governments implementing and moving off-line services online, providing greater digital services and doing it right by coming to you and saying, “Let's address privacy concerns”? Can we point to any Canadian example where there's been a service that's gotten it right? Take your time.

Voices: Oh, oh!

Mr. Daniel Therrien: In the spirit of being optimistic and positive, I would say that the Estonian model is interesting to look at from that perspective. It has many positive features. The devil is in the details, obviously, but it's not a bad place to start.

Mr. Nathaniel Erskine-Smith: All right. Thanks very much.

David.

Mr. David de Burgh Graham (Laurentides—Labelle, Lib.): Thank you.

I think data is easier to share than time, but we'll do what we can.

[*Translation*]

I would like to understand how we can define the parameters for the permission that people give. On Tuesday, I used automatic vehicle licence plate readers as an example. When a car goes by, the reader records the plate number. That is being done by the government. We provide that data in a way that is not really voluntary, given that we have no other choice.

If departments or police services all over the country use that data without really having obtained people's permission to do so, how can we determine whether they have given their consent? Where do we draw the line?

Mr. Daniel Therrien: I will assume that your question is based on the principle that this is information in the public domain. Licence plates are public, in a sense, because the cars are travelling on public roads. People—the government, but companies too—rely on the public nature of that environment to collect data and then to use them in a way that does not see them as personal information. In that case, the rules on the use and disclosure of that information are more permissive.

Mr. David de Burgh Graham: At each stage of a trip, the plate number can be read, revealing who it belongs to, where they live, and their record. Even if the data is not collected every time, individuals can be followed from one end of the country to the others, and their travels known.

That is not what licence plates are for, but, if we say they are in the public domain, are we allowed to use the data in that way? The United States is already doing it.

● (1550)

Mr. Daniel Therrien: We have to be careful in calling this information public. As you have just said, it is still possible to identify the person associated with a car, their behaviour, and so on. So, even if the information is called public, we have to wonder whether the information is actually personal, and what authority a given department has to collect it. It varies from department to department. Even though the information is in the public domain, collecting it has to be linked to a mandate of the department in question. That is a very important condition in the current legislation. It could be made stronger, along the lines of some recommendations we made in connection with amending the Privacy Act.

In summary, we have to be careful with data in the public domain. We have to make sure that each department collecting and using the information actually has a mandate to do so.

Mr. David de Burgh Graham: Thank you.

[*English*]

Do I have any time left?

The Chair: You're out of time.

[*Translation*]

Mr. David de Burgh Graham: Thank you.

[*English*]

The Chair: We'll go to Mr. Kent for the next seven minutes.

Hon. Peter Kent: Thank you, Chair.

It's good to see you again, Commissioner, and your partners today at the table.

Given the significant differences between the Estonian model and Canada today.... The digital identity in Estonia covers literally a person's entire lifetime, not just their health and tax information but their education.... It covers just about every aspect of their daily life.

From reading your remarks, you seem to see the first stage of digital government, should it come to Canada, as beginning at the federal government level alone. Is there any practicality in trying to get into those areas where there is a sharp divide and no overlap with provincial and municipal jurisdictions?

Mr. Daniel Therrien: A very significant difference, of course, between Estonia and Canada is that we're a federal state whereas they're a unitary state. That creates certain difficulties in Canada in setting up a system, difficulties of various orders. These could be technological, but there are also different administrations and different legislation. I don't think it's inconceivable that there could be a system that would share information between the federal and provincial governments, but given the complexity of the Canadian federal state, it's probably more practical to start at one level.

Hon. Peter Kent: Did you observe or have you read the transcript of Dr. Cavoukian's and Dr. Geist's appearance before committee this week?

Mr. Daniel Therrien: Yes.

Hon. Peter Kent: Could you offer some of your general observations? Dr. Cavoukian had some very significant concerns.

Mr. Daniel Therrien: I'll put it in my terms.

I think the Estonian model is interesting in that the risk of digitized government services based on a common digital identifier, in the worst-case scenario, would be that the government, whether only the federal government or governments generally, would have a single profile of that individual. That is, of course, very difficult to reconcile with privacy.

One of the apparent virtues of the Estonian model is that the data is not centralized. It continues to reside in a large number of institutions, and there's a technological pathway with appropriate legal authority authorizing the information to be reused from one department to another. The decentralized aspect of the Estonian model, I think, at first blush, seems a positive feature that reduces what would otherwise be a risk.

You mentioned concerns that were expressed.

Hon. Peter Kent: Yes.

Mr. Daniel Therrien: Can you be more specific?

Hon. Peter Kent: I don't have the transcript in front of me, but basically, as I read many of the remarks that Dr. Cavoukian returned to, the cybersecurity of that digital information as it moves from the several repositories to whoever is requesting or accessing that information is vulnerable. The guarantees of absolute security do not yet exist.

● (1555)

Mr. Daniel Therrien: There is no question that technological systems are vulnerable to breaches. I'm not sure there will ever be a system that is free of that risk. I think, legally speaking, if digital services occur, it's important that there be a legal obligation for government to apply strong technological safeguards. Technologically, in Estonia, as you know, there are blockchains and encryption. These are state-of-the-art systems. Do they guarantee that there will not be breaches? No.

Hon. Peter Kent: In your opening remarks you mentioned trust and consent. Again, a significant difference between Estonia and Canada is a very compliant population after the breakup of the Soviet Union, and a very forceful new democracy determined to create digital government from scratch.

Given Canadians' natural skepticism and generational cynicism about the digital world, and given Cambridge Analytica, Facebook, Aggregate IQ, all of the scandals and now controversy over Sidewalk Labs and people's concern about exposure, privacy, personal content, who owns what and how it's accessed, do you think that on that level alone it will be an uphill battle to get the consent of Canadians for this kind of digital government in any reasonable period of time? I'm talking about perhaps a decade, in our lifetimes.

Mr. Daniel Therrien: I think Estonian officials mentioned that even in Estonia, the systems are not implemented overnight. There are a number of steps.

I think technological safeguards are crucial. Legal safeguards are crucial. I will say that probably incremental implementation, where government has a chance to demonstrate that the system deserves trust, may lead us towards trust in the population. There's no question that currently, Canadians are concerned that their privacy is not being respected.

Hon. Peter Kent: Thank you.

The Chair: Thank you, Mr. Kent.

Next up for seven minutes is Mr. Angus.

Mr. Charlie Angus: Thank you, Mr. Chair.

Mr. Therrien, it's always a pleasure to have you at our committee.

I want to follow up on your final statement about the question of trust and whether or not Canadians should be expected to trust a system such as this.

On my beat in this file over the years, I've seen that every year we have data breaches. Some are extremely significant data breaches, such as the loan information of a quarter million or more students, and recently, 80,000 individuals compromised through CRA.

In your work, is the number of breaches changing because technology is changing? Is it a standard...? Year in and year out, are we seeing some pretty significant, plus smaller, breaches? In terms of government departments, are you seeing much of a change?

Mr. Daniel Therrien: I would not say that we're seeing significant improvement in these matters. It's a huge challenge to build that trust; there's no question.

I'll use an example, because I think it's telling on many levels. As you know, the government implemented a pay system called Phoenix that was criticized on a number of levels. We, the OPC, investigated the security and privacy safeguards that were in place, or not, with respect to the Phoenix system. One of the very concerning things we found during that investigation was that there was a deliberate decision by government officials not to put in place strong monitoring of who had access to personal information in the system, because it would be costly, would delay the system, and so on and so forth.

Directly to your question, I don't see many improvements. I would say it is absolutely essential that before these systems are implemented more broadly—to go back to attitudes—that government officials have an attitude of ensuring that safeguards are in place before the systems are implemented.

● (1600)

Mr. Charlie Angus: I thank you very much for that response. It leads me into where I was concerned.

I've been here 15 years. I see my colleagues on the other side and they're flush with the hope of new believers that we have finally come to the kingdom of salvation and government will work; whereas, over the years I've become a skeptic, an agnostic.

Some hon. members: Oh, oh!

Mr. Charlie Angus: I'm like the St. Thomas of government operations. I've sat on committee after committee where we were sure that bigger was better, that government always.... Whenever they were looking for who was going to get the contracts, they wanted to go as big as possible. Bigger was not better. Bigger was much more expensive. Bigger was always tied with deals, and the deputy ministers and who got the deals and who didn't.

Then we had Phoenix. I guess I would turn around to citizens in my riding and say, “Look at Phoenix. Do you trust?” In terms of the safeguards that need to be in place, would you not think it would be an extremely complex set of safeguards, that we would be able to assure Canadians that they can trust all their financial information, all their personal information, their life history with a department or a government that has, year in and year out, serious breaches in many and almost all of the serious, major departments?

Mr. Daniel Therrien: It's complex, but I would say it's within human capacity. It probably speaks to the need to implement this incrementally because systems cannot be changed overnight, so you start incrementally, I think. Of course, I would start with...there is no choice but to make government services digital for all kinds of reasons, including to improve services to the population. It's not a question of not doing it because it's too complex and daunting, but in implementing this policy there should not be short shrift given to policy safeguards, legal and technological safeguards.

Mr. Charlie Angus: Thank you for that.

Certainly, I know the people I deal with would prefer to have people actually answering phones if they had questions as opposed to getting their digital data quicker. We will always see them go with digital solutions as opposed to having people answer the phones.

I'm concerned about whether this is a one-way path or a two-way path. If I want to find my CRA information and I have a digital card, I can find that. It was suggested by one of my Liberal colleagues that it would be a great way for government to contact citizens.

To me, that's very concerning. If I am obligated to do everything online, if I have to give all this information online, there's the necessity, I think, of saying that this is so I can obtain services I want, but not necessarily for government to be able to contact me about what they want.

Do you see that if we have a two-way communication, it changes the nature of this, and the privacy rights of citizens become much more at risk from potential abuse?

Mr. Daniel Therrien: The situation you describe is exactly why I say it is essential to look very closely at the legal framework within which either data will be shared from one department to another, or a second department will be able to reuse data that the first department has à la Estonia.

It starts with the right legal framework, which limits the circumstances where a department calls on a citizen because another department has offered a service. That's extremely important. We have rules already in sections 4 to 8 of the Privacy Act. Yes, they can be reviewed, but it's not a bad place to start either. That's an important part of the foundation. Then I think the technology follows the principles that have been adopted with safeguards ensuring that, technologically speaking, data banks cannot talk to each other unless there's a legal authority to do that.

It starts with a well-defined and well-thought-out framework. Call it sharing. Call it reuse of information.

● (1605)

Mr. Charlie Angus: Thank you very much.

The Chair: Thank you, Mr. Angus.

Next up for seven minutes is Mr. Saini.

Mr. Raj Saini: Good afternoon, Mr. Therrien. It's always a pleasure to have you here. I think you're the witness who visits this committee the most so that's great.

You made a submission to ISED dated November 23. I read it through. It was very interesting. One thing you did write was, “It is not an exaggeration to say that the digitization of so much of our lives is reshaping humanity.” I would go even further that once that march towards technology has started, it's very difficult for anybody to stop it. Eventually it will succeed.

I know the model we have been using is Estonia, but if you look at Estonia right now, you see there are 1.3 million people, four million hectares of land, and half of it is forest, so broadband connectivity is not really a big issue there. When we look at Canada right now and the latest UN survey on leading countries in e-government development, we see that we rank 23rd, so eventually the world is moving in this direction.

You indicated in the notes I have read that privacy is a big concern for you. There has to be a point as to where we start from and what the objective is. The majority of countries, especially advanced countries, are moving towards more digitization of government. Let's leave Estonia aside for a second. Where do we start from?

I'm going to frame this in two ways. The one frame I had is because in Estonia you have two levels of government. In some cases, we have four levels of government. How do we protect privacy? As Mr. Angus said, people want to have security of their data, but different governments do different roles. It's not one government that's a repository. The provincial government deals with health. The federal government has the CRA. How do we protect the privacy of Canadians going through different levels of government? How do we make the system interoperable among different departments within one level of government?

Mr. Daniel Therrien: I think an appropriate starting point might be to define what the specific circumstances are where government believes that it is inhibited from delivering efficient services because of what are often referred to as silos between departments that prevent information sharing. What are the practical problems? What do citizens actually want other than more efficient government generally? What kinds of services cannot be delivered efficiently in a timely way because of legal and bureaucratic impediments? I think that would be a start.

Mr. Raj Saini: Also, the working theory in Estonia is that the public or the citizens own the data. It's up to them how they dispense that data and who they allow it to be shared with.

If we go one step forward, if we start off with the public sector, obviously the private sector is going to have some involvement, whether it be bank information or other information. If the private sector has different technology and the public sector has different technology.... One of the examples that has been given is blockchain technology.

One entity is governed by PIPEDA and another entity is governed by the Privacy Act. How would you mesh both of them together? Where would the touchpoint be where you could allow the public sector and the private sector to maintain privacy but also to maintain their own jurisdiction?

Mr. Daniel Therrien: I'm not a technologist, although now I'm gaining a bit more knowledge about technology after being in this position for a few years, but I think we're back to an incremental approach. The systems will be interoperable not overnight but gradually. Technology is a means. I would start with what government wants to do and what the impediments are to efficient services. Then I would determine what the required technology is to get you to the proper place.

● (1610)

Mr. Raj Saini: Obviously, the digitization of government is going to move forward. Whether we do it quickly or slowly, it's going to go forward. What role should there be and where should the insertion point be for the Office of the Privacy Commissioner in terms of the leading the way, making sure that the system has not been developed? Then afterward your office would come in and say there are points here that we have difficulty with.

Where do you see your insertion point? You're talking about technology. You're talking about privacy. You're talking about in some cases portability. You're talking about different levels of government. You're talking about interoperability within government. Where do you feel your office should insert itself to make sure that this becomes an effective approach?

Mr. Daniel Therrien: I will use the word “proactivity”, which I have used in this committee previously with respect to Privacy Act reform.

We have approached current officials to ask them to give advice as departments develop their individual strategies. I think that's part of it. If laws are amended, we should be consulted in the development of laws. Once laws are adopted, we should have the stronger powers that we have sought to ensure that legal privacy principles are actually being implemented. It's going to be a long journey.

My answer is that with our limited resources we're willing and able to play as proactive a role as possible. We will not define the objectives. Government will define the objectives, but we are able within our means to give advice as early as possible, and once systems are adopted, to play an oversight role with legal powers to play that role.

Mr. Raj Saini: I have a final question.

You're talking about different actors and players. Do you think it would be better to start at a baseline where you had government, private sector, public sector, technologists sitting together to form a pathway going forward so that everybody is on the same page? In that way it would be done in step, in line, and proactively but intermittently in a way that makes sure that if iteratively there are changes that have to be made, they won't be made at the end of the development of a system, but at the beginning where it goes step by step.

Mr. Daniel Therrien: I think there's a place for that kind of overarching discussion at a level of principles, be they legal, bureaucratic, operational or technological. But in terms of implementing these, on balance, I think it's going to be done incrementally.

Mr. Raj Saini: Thank you.

The Chair: Next up for five minutes is Mr. Gourde.

[*Translation*]

Mr. Jacques Gourde (Lévis—Lotbinière, CPC): Thank you, Mr. Chair.

Thank you for being here, Mr. Therrien.

Do you think there is an economic study on digitizing data in Canada in the future, so that Canadians can have some idea about the issue? Is it in the millions, the billions?

Mr. Daniel Therrien: I did not hear the start of your question. Are you asking me about the cost of digitization?

Mr. Jacques Gourde: Is there a study that establishes the cost of a digital world that will make sense in the future? We know that the firearms registry cost almost $2 billion, just to enter the data on long guns. Imagine how much it could cost to enter digital data for all of Canada.

Mr. Daniel Therrien: To my knowledge, there is no such study. It would be quite the undertaking to do one.

One of the reasons why I am in favour of the government digitizing its services is that health care, for example, could be improved. We may have to invest in technology, for example, but there would be a return on the investments, since health care would be more efficient.

To my knowledge, no such study exists. First, it is difficult to imagine the future without digitization. Second, even though there would be a significant cost, there would surely be a return on the investments.

Mr. Jacques Gourde: Our departments' services are already digitized, but it is done piecemeal. Services are already being provided to Canadians, but everyone does their own thing.

● (1615)

Mr. Daniel Therrien: Yes.

Mr. Jacques Gourde: Some things could probably be kept. What should be our approach? We could probably provide Canadians with many more services without throwing the baby out with the bathwater or starting everything from square one.

Mr. Daniel Therrien: I agree with you. That is why I talk about an approach in stages, where systems that work would be maintained. The government should identify where things are not working so well and make improvements. That does not mean opening everything to question and starting again from zero, technologically at least.

Mr. Jacques Gourde: In an ideal digitized world, which of Canadians' confidential or more sensitive information would be less protected in that new world?

Mr. Daniel Therrien: The government has all kinds of extremely sensitive information. I have just talked about the area of health. Medical information is among the most important. Identification can depend on biometrics. This information is very sensitive. The government has no choice but to collect and use sensitive information that is the very essence of privacy. All the information that the government has will obviously contain sensitive data, such as financial information. As a result, the protections must be at a very high level.

Mr. Jacques Gourde: Thank you, Mr. Therrien.

Mr. Chair, I just want to make a brief comment. When discussions are going on at the back of the room, it is tiring for those asking questions. Perhaps we could ask those who need to hold the discussions to leave the room. If the discussions are necessary, then let's stop the meeting completely. Personally, it bothers me.

[*English*]

The Chair: Yes, I think it has subsided now. I ask everybody in the room that if you're going to have a conversation that's loud enough to hear from the table here, to move into the hallway.

Thank you.

Go ahead, Mr. Gourde.

[*Translation*]

Mr. Jacques Gourde: That's it for me. Thank you.

[*English*]

The Chair: Okay, thank you.

Next up for five minutes is Mr. Baylis.

Mr. Frank Baylis (Pierrefonds—Dollard, Lib.): It's good to have you back, Mr. Therrien, because you're very private and we don't get a lot of information.

There are a couple of statements that I would like to refute. One is that Canadians are afraid of technology or digitization. I point to the statistic that 85% of people do their taxes online. They're not forced to; they have the right to do it on paper. They choose to do it online for all types of efficiency reasons.

Have you any evidence, other than what's been stated, that Canadians are anti-technology or against digitization per se?

Mr. Daniel Therrien: I don't think I've said that Canadians are concerned with the use of technology.

[*Translation*]

I did not say that they distrust technology.

Studies consistently show that Canadians are concerned that their privacy is not being protected, in both the public and the private sectors, and that they do not have control over their information. That is not to say that they do not use technology or that they distrust it. It is rather that they believe that their privacy is not being sufficiently protected, by the public or the private sectors.

Services have to be digitized, but with the use of different means, legal, technological or whatever, to make completely sure that the information is secure.

Mr. Frank Baylis: You are making quite an important distinction.

[*English*]

Although there is the ability to be abused through digitization, people were stealing identities and doing all this long before we had computers and digitization. People aren't against digitization, but they just have a concern about their privacy and want to ensure that if we do go that route, we do what we can to protect their privacy. Is that what...?

Mr. Daniel Therrien: Yes, there was theft of information before, but clearly with digitization, the scope of the consequence of a breach is magnified greatly.

● (1620)

Mr. Frank Baylis: It is right now. That's true.

Ms. Cavoukian, who is an expert in this area, testified at the last session. She made the argument that security and privacy are not incompatible. It's not one or the other. In fact, we have to stop thinking this way. If things were done correctly, we could actually have more privacy with better security as opposed to always saying, "Well, if we had a lot more security, we'd lose on this side or that side."

Do you have thoughts along those lines?

Mr. Daniel Therrien: I agree. It's not a zero-sum game between privacy and security, nor between privacy and innovation, nor between privacy and improved service delivery. It is possible to have all of that, provided that the systems, including the legal systems, are designed properly. That leads me to privacy by design, which is an important concept that should be in the law but should also be applied on the ground by the bureaucracy, by departments, in the delivery of services

Mr. Frank Baylis: In a way, we find ourselves right now where we've heard comparisons to the wild west or whatever. When something is new, the people go out, prospect, run, grab territory and all that, and then afterwards the law comes in and we slowly structure things around it. We're living in an era right now where there are not sufficient laws certainly in the digital world, and we have to catch up, if I can say that. However, I would ask you to underline that we cannot, as some people say, go back or even just stay static. We have to go forward, but we can go forward with what Ms. Cavoukian came up with as a concept, which is rather new, and that is privacy by design, so that we start to think about privacy as we're designing the next one.

What are your thoughts there?

Mr. Daniel Therrien: I agree. I totally support the principle of privacy by design. I would say this with regard to the fact that digitization is something that will necessarily happen—that's true—but privacy by design means that, again, the way in which we proceed needs to be thought out seriously and rigorously.

One of the issues to be considered is the role of the private sector in the delivery of services by government. You mentioned the wild west. You're well placed to know there are important problems with the way in which certain corporations are handling the personal data of individuals. Improving government services is being thought out in terms of relying on technology owned by the private sector in the delivery of services. That's fine, but the way in which these services will be delivered, calling on the private sector—say, the Alexas of this world—the government needs to be very careful as to how this will happen for many reasons, including who owns or controls the information that goes through Alexa when a citizen is asking for services from its government. What happens to that information? Is this information under public control or private control? Is it monetized or not? These are very important and fundamental questions.

Mr. Frank Baylis: Thank you.

The Chair: Thank you, Mr. Baylis.

Mr. Kent, you're next up for five minutes.

Hon. Peter Kent: Thanks.

Commissioner, this committee has tabled three reports with the government over the past year or so recommending in each of those reports that your powers be expanded, that you have order-making powers, that there be more serious and significant penalties for violations, that in terms of the act itself, the government consider the GDPR and upgrade, renovate, and stiffen Canadian privacy regulations from the very barely acceptable level we're at today.

Would you recommend that your office be a direct participant, a hand on the pen at the table, as the design of digital government is considered and written? In other words, do you think it's essential that the Privacy Commissioner be a key partner in any project going ahead, either in the early stages or certainly in later stages of digital government?

● (1625)

Mr. Daniel Therrien: We have value to add, for sure, and we have made our services available to government. Sometimes they have accepted that offer. Is it necessary? That might not be for me to say, but I do generally believe that we have value to add and that systems that would consider our recommendations have a better chance of being privacy sensitive.

Where it is not a question of choice is at the back end, where once a law is designed that, for instance, talks about the conditions under which data will be shared between departments, there needs to be a strong regulator to ensure that these conditions are respected. That is the OPC.

Hon. Peter Kent: If digital government is the property of the government and if there was hypothetically a significant and serious data breach, a damaging data breach, involving the privacy of Canadian citizens or anyone in the digital government system, would you think it would be the Privacy Commissioner that would level penalties against those responsible for that data breach? How would that work if government is actually the corporate controller of that system?

Mr. Daniel Therrien: You're raising the issue—

Hon. Peter Kent: It's about accountability.

Mr. Daniel Therrien: Okay, so government needs to be accountable in the way in which it manages information in relation to citizens. We, the OPC, are well placed to ensure that in individual circumstance the government is called to be accountable and that a breach of data be identified and remedied.

Does it need to lead to a financial penalty? I'm less certain of that in the public sector, but there needs to be somebody to identify violations of the law and to ensure that these violations are remedied, and we are well placed to do that.

Hon. Peter Kent: The Estonian model has repositories. As you said, there are many silos that are hooked into the central system and the single citizen chip. There will almost certainly be competition for financial gain by a variety of parties to participate in digital government. Neil Parmenter, the president of the Canadian Bankers Association, in a speech that I attended last month, made a point of saying Canada's banks are trusted. There is the double-factor log-in, and he expressed an interest in the banks being a central participant in digital government. Do you have any thoughts on that type of proposition?

Mr. Daniel Therrien: It is true that banks offer services that, compared to others, are well protected. I have no problem in principle with banks or other reputable organizations, private organizations, being responsible, say, to manage the common identifier. That's one element of the system. What type of information they actually get when the government delivers services to the citizens, for me, is a different issue, but in terms of managing a secure common identifier, banks are probably well placed to do that.

Hon. Peter Kent: Thank you.

The Chair: Thank you, Mr. Kent.

Last up is Monsieur Picard.

[*Translation*]

Mr. Michel Picard (Montarville, Lib.): Good afternoon, Mr. Therrien.

Let me put something to you; I would like to know your opinion.

I am not criticizing the work we have done at all. I have thought for a long time that the committee has been doing valuable, excellent work. However, I want to suggest to you another way of looking at things.

We have been studying the protection of personal data for six or eight months. But I feel that we are spinning our wheels and getting nowhere, because we have not managed to define the problem we are trying to fix, by which I mean defining what personal information is. Let me explain.

People panic at the idea that a licence plate can be read, pretending that it is private. But all that plate can do is identify the vehicle on which it is mounted, not the person at the wheel. In the same way, an IP address does not reveal the identity of the person at the computer keyboard, just where the computer is located.

People gladly provide a lot of personal information. For example, you may remember when, in the first video clubs, we did not hesitate to provide our driving license numbers so that we could rent movies.

The reason why I feel that we do not want to touch the problem of defining personal information is that most of the witnesses we have heard from for almost a year have replied that the best way to protect our personal information was not through technology, but through transparency. Companies understand that people are ready to give them almost any personal information but, in return, they have to commit to telling them what they are going to do with it. So that means that the range of the data that you are ready to provide to anyone at all is not defined. As a result, if we are not able to define the problem that we want to fix, it will be difficult to define the measures that we want to take. Why not just simply stop right there and prevent any data transactions? If someone wants to conduct such a transaction, they would have to communicate with you to find out how to manage the information that is being communicated. That is the first part of my question.

● (1630)

Mr. Daniel Therrien: In law, I am afraid I must tell you that you are wrong when you suggest that IP addresses are not personal information. The Supreme Court decided otherwise in a judgment some years ago. Since an IP address can be linked to an individual, it is personal information that must be protected as such.

With licence plates, the issue is somewhat not quite the same. After all, 800 people do not drive my vehicle, just my wife and I. Perhaps that is personal information as well.

So personal information is defined. It is pretty simple; it is any information, including a number, that can be linked to an identifiable person. We can discuss it, but I am inclined not to accept your premise.

Is transparency part of the solution in protecting privacy? Yes, it is part of the solution but it is far from the entire solution. You can be transparent, but you can still damage someone's reputation. However, transparency is part of the solution.

This certainly is a complex question, and if we are having difficulty moving forward, it is because it is complex on a number of levels, including conceptual and technological. That is why, more recently, I have focused on privacy as a human right. So let's start with basic principles.

When I say that privacy is a fundamental right, it is a concept that should be recognized, not only in the law, but also by government bodies that, day after day, implement technological and other systems to collect data and to administer public programs, including by technology. That brings us back to the importance of protecting privacy from the design stage, a concept that we should always keep in mind. If we have a choice between providing a service in a way that endangers privacy and providing the same service differently, but just as effectively, in a way that protects privacy, the concept of protecting privacy from the design stage tells us that we should choose the latter option.

All these privacy issues may seem nebulous, but, in law, what constitutes personal information is quite clear. We have to keep in mind which aspects of privacy we want to protect, so that we make sure that it is protected in government activities and in legislation.

● (1635)

[*English*]

The Chair: Thank you, Mr. Picard.

I have Mr. Angus for the last few minutes. I was asked to split some time by two other members who haven't had a chance to ask a question. We'll do that following Mr. Angus, and then we'll go to the motion that was brought up before.

We'll go to Mr. Angus for three minutes.

Mr. Charlie Angus: Thank you, Mr. Chair.

Thank you, Mr. Therrien.

We began a study much earlier in this Parliament on a data breach with Cambridge Analytica and Facebook. Since then, I sometimes feel we've become the parliamentary committee on Facebook. We followed them halfway around the world trying to get answers, and we're still being buffaloed, and I think we'll invite half the world to come here to meet with us again in Ottawa when it's a little warmer to maybe get some more answers from Facebook. But it seems we go week in, week out with new questions and seemingly a continual lack of accountability.

I want to ask you a specific question, though, whether or not you've looked into it. We had the explosive article in The New York Times about the privileges given to certain Facebook users, to be able to read the personal, private messages of Facebook users. They mentioned that RBC was one of them. We've heard from RBC. They said they never had those privileges, that they never did that. The Tyee is now reporting that Facebook has told them that RBC had the capacity to read, write and delete private messages of Facebook users who were using the banking app.

Have you looked into that? Do you think that requires follow-up? Should we take RBC's word for it? Should we, as a committee, be considering this as some of our unfinished business on the Facebook file?

Mr. Daniel Therrien: The short answer is yes, in two respects.

When the British parliamentary committee published the documents from Six4Three, we saw references to the Royal Bank, and we considered whether to look at this particular aspect in the context of our investigation into Facebook and AIQ. As we were doing this, we received complaints from individuals on whether or not the Royal Bank was violating PIPEDA in some way in receiving information in that way. So that question is the subject of a separate investigation.

Mr. Charlie Angus: Just to be clear, you received complaints about RBC violations—

Mr. Daniel Therrien: About RBC's alleged role in receiving information from Facebook, allegedly in violation of PIPEDA.

Mr. Charlie Angus: Okay. From your knowledge of this back channel that was given to certain preferred customers with Facebook, would it have been possible to read the private messages of Facebook users if you had access to that?

Mr. Daniel Therrien: I can't comment on that. We're investigating. We'll find out for sure.

Mr. Charlie Angus: You're investigating. Okay, fair enough.

Thank you very much for that.

The Chair: Thank you, Mr. Angus.

We're going to go to Ms. Vandenbeld for two and a half minutes, and then....

Mrs. Mona Fortier: She'll take it all.

The Chair: Okay.

Go ahead.

Ms. Anita Vandenbeld (Ottawa West—Nepean, Lib.): Thank you, Mr. Chair, for your indulgence on my getting the last question. It's very important and interesting testimony.

I'd like to pick up on this idea of ownership and consent in the context of government. If I go on Air Canada, and they ask me for my email and cellphone number so they'll text me when my flight is delayed or anything, I have a choice to do that. However, there are things in government where you don't have a choice. You have to provide information. Your taxes are required. The idea of consent immediately has a different implication when something has to be provided.

In that context, how do you see consent, or even who owns that data? If I go to Air Canada, I can take my profile off. I have a choice. But with government, if there's a criminal record, you can't say you want to delete this or change that. The information no longer really belongs to the person.

Where does ownership and consent go when you're dealing with government?

● (1640)

Mr. Daniel Therrien: You're absolutely right that in a government context, consent is not always required for a government to collect information. The situation doesn't arise in quite the same way. We have rules already in the Privacy Act for this.

One rule is that, as it stands, government should collect information, to the extent possible, directly from the person interested in the information, either with or without consent, say, in a law enforcement situation. The principle is to collect directly from the individual, which then leads to questions around what's on social media or potentially publicly available. That's a difficult area to navigate under the current act. But the first principle is to collect normally from the individual concerned, with or without consent. That's not the quite the same situation as for the private sector. I agree that consent is not always required.

Ms. Anita Vandenbeld: Given that, we heard that government is using things like predictive analytics and could also use more in the future. I think the example that was given is that CRA can even use some form of AI with predictive analytics to determine where fraud is more likely to be occurring, so they can target and look at those sorts of things.

However, if you think of the concept of privacy by design, that is specifically saying that data is used for the purpose for which it's collected. If you're providing information to CRA about your taxes, but CRA has a mandate to investigate tax fraud, it may not necessarily be the purpose for which it was collected, but it might be a legitimate use of the information by government. That's just one example.

In this world of more predictive analytics and more AI, where does the idea of privacy by design fit with that?

Mr. Daniel Therrien: In a tax context, there is information that CRA obtains directly from the taxpayer. It is possible that the CRA looks at social media and other environmental information to gather intelligence and may put all of this information towards artificial intelligence. It's important. Data analytics is a new reality and it has many advantages.

However, AI systems need to be implemented in a way such that the information that feeds the system is reliable and has been lawfully obtained, so that leads to certain consequences. If CRA looks at information on social media, and let's assume for a second that it is truly publicly available, that says nothing about the reliability of the information.

To answer your question, in an AI context, privacy by design ensures that AI is implemented in such a way that the information that feeds the system, first, has been lawfully obtained, second, is reliable, and third, does not discriminate on the basis of prohibited grounds of discrimination, but is based on objective factors of analysis.

Ms. Anita Vandenbeld: It's also been suggested that for many purposes we would de-identify data before you would go through this. Is that something you think is feasible?

Mr. Daniel Therrien: That is preferable but not always possible. It's conceivable that AI could work with personal information, but the preference would be to start with anonymized information.

Ms. Anita Vandenbeld: Thank you.

The Chair: Thank you, all.

Thanks to the commissioner and his staff for appearing before us today. It's always thoughtful and this issue seems to be ever growing, so again, thanks for coming today.

Mr. Daniel Therrien: You're welcome.

The Chair: For the rest of the committee, we're going to stay for a minute, just to address the motion that was presented prior to Mr. Therrien's testimony.

We'll go back to Mr. Kent, first, and then to Mr. Angus.

Hon. Peter Kent: Thank you, Chair.

I understand the Liberals would like 48 hours to consider the request, so in the interest of collegiality, I would accept that 48 hours.

However, I would put forward a motion saying that this original motion from today be dealt with as the first item of our next meeting.

The Chair: Go ahead, Mr. Angus.

Mr. Charlie Angus: I am absolutely outraged by my colleague's collegiality, so I am going to have to talk to my colleague beside me to decide if we are going to filibuster.

● (1645)

The Chair: It sounds like it's been a discussion that's been rather loud during the committee meeting, so next time, I would ask that it be a little quieter. It sounds like we're going to deal with this on Tuesday, so have a good weekend, everybody.

Yes, Mr. Angus.

Mr. Charlie Angus: I have one other element. We were supposed to discuss my motion today, which is that we are going to have to plan for a parallel study to happen. Nathaniel has asked to be able to work on the language of my motion in advance of a public meeting.

Just in the interest of being really collegial—you get one out of the whole four years in Parliament, and this is it and you can put it in your pocket.

Mr. Frank Baylis: We can put that on Twitter.

Mr. Charlie Angus: Yes, you could put it on Twitter. I'm being collegial today.

I will come back with some language that hopefully works for everyone and I'll pass it to Peter to look at it.

Thank you.

The Chair: Thanks, everybody. Have a good weekend.

The meeting is adjourned.