HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 027 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, October 6, 2016

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Thursday, October 6, 2016

● (1100)

[*Translation*]

The Vice-Chair (Mr. Joël Lightbound (Louis-Hébert, Lib.)): Greetings, everyone.

Welcome to this meeting of the Standing Committee on Access to Information, Privacy and Ethics. The Chair, Mr. Calkins, is not here today, so I will be replacing him. Consequently, this meeting of the committee will be chaired in French.

I'd like to thank the various witnesses for being with us today. Chantal Bernier, of Dentons Canada, was also with the Office of the Privacy Commissioner of Canada for six years. Monique McCulloch is with Shared Services Canada, and Maxime Guénette and Marie-Claude Juneau are with the Canada Revenue Agency.

Each group will have 10 minutes to give a presentation. This will be followed by a question period, in which the committee members can ask questions.

I will begin based on the order I have before me. Which means you begin, Ms. Bernier. You have the floor.

Ms. Chantal Bernier (Counsel, Privacy and Cybersecurity, Dentons Canada): Thank you, Mr. Chair.

First of all, I'd like to express what a pleasure and honour it is to be back before you today. It's a bit of a homecoming. I'm truly honoured to be able to help inform your debate on a topic of such importance.

I will be giving my presentation in both official languages. I guess 27 years as a public servant has made a lasting impact. So I will start in French, but continue my remarks in English.

I should tell you from the outset that I'm in total agreement with the recommendations of the Privacy Commissioner of Canada concerning the reform of the Privacy Act

To avoid exceeding my allotted time, I have chosen to expand on what I consider to be the priority recommendations. Naturally, during the question period, I will be happy to elaborate on any recommendations I have not mentioned due to time limitations. Without further delay, I will move on to the first point I wish to make.

My first recommendation is about the requirement for written agreements governing the sharing of personal information. In support of this recommendation, I refer you to two documents: Justice O'Connor's report as part of the Commission of Inquiry into the Actions of Canadian Officials in relation to Maher Arar; and the special report entitled "Checks and Controls" that I tabled in Parliament on January 28, 2014, with the assistance of the wonderful staff at the Office of the Privacy Commissioner, and with input—this deserves to be emphasized—from five experts in national security.

Let's begin with Justice O'Connor's inquiry report in the Arar matter.

In his report, Justice O'Connor concluded that by sharing personal data about Mr. Arar with foreign authorities, Canadian government authorities had contributed to the torture of an innocent person. In the hope preventing this from happening again, he recommended that Canada better control the transfer of personal information to foreign agencies. This shows how topical the Privacy Commissioner's recommendation is.

In the introduction to the special report that I filed on January 28, 2014, the experts we consulted mentioned the levelling of territorial boundaries, be they national or international, as a decisive change in the public security context. This change necessitates the sharing of personal information.

Given this convergence of necessity and risk, I believe the requirement for written agreements to better govern this sharing is needed for two major reasons: the protection of fundamental rights, and the accountability of government agencies in protecting these fundamental rights. The Commissioner's recommendation is therefore very relevant, and even urgent, in this regard.

● (1105)

[*English*]

Let's move now to the second recommendation that I would like to underline in my list of priorities. It is restricting collection to a government program by relevance to activity.

On this front, I would actually like to go further than the Privacy Commissioner. I fully support his proposal; however, I would prefer to tie the requirement of necessity not to the program or activity, but to the Canadian Charter of Rights and Freedoms. The reason is that it would be stronger protection.

Indeed, let me show you through a concrete example in the work that I did for nearly six years how the linkage outside the program or activity is superior.

In 2009 at the OPC we received a privacy impact assessment from the RCMP to roll out a program whereby a camera mounted on the cars of the RCMP would pick up licence plates. Automatic licence plate recognition was the name, and it would retain information about, let's say, non-executed warrants or interventions that had to be effected and could not be effected, a suspended driver's licence, for example.

It would keep the data that did have a match in the police database for two years, and it would keep the data that did not have any match for six months. In other words, the data—meaning the licence plate recognition of Mrs. So-and-so, who happened to be doing her groceries at this time at this supermarket—would be held for six months, in spite of no contravention of the law whatsoever. We questioned that, and the RCMP said, “Well, it's part of the program”, to which we said, “But it does not meet the standard of necessity under the charter, and the charter has precedence over every other law”. The RCMP indeed took that out and did not retain the innocent person's information.

That, to me, truly shows that there is superior protection where you link it to the charter, rather than embed it in a justification of the program.

The third priority I will underline is to require federal institutions to consult the Office of the Privacy Commissioner on legislation and regulations with privacy implications before they are tabled. To me, the logic of this recommendation lies, first of all, in the role of the commissioner as an agent of Parliament, and second, in the fundamental nature of the right to privacy.

Let's look at the commissioner's role and status. The Privacy Commissioner is an agent of Parliament. What does that mean? That means that he has been invested with the protection of a value so important to Canadian identity and democracy that he is placed above political partisanship and reports directly to Parliament.

Because of this status, and the fact that privacy has been entrusted to an institution with this status, it is completely logical that the commissioner be consulted about legislation or regulations prior to their being tabled, to ensure they are privacy-compliant.

The example I will use here, which I feel clearly illustrates the advantage of this recommendation, can be found in a series of bills that either died on the Order Paper or were withdrawn or adopted with reservations regarding lawful access. These bills were so deficient in terms of compliance that they did not survive political wrath and proved to be untenable. They led to acrimonious debates and undermined public confidence in government institutions. Prior consultation with the Privacy Commissioner, I believe, would have provided for a dialogue between the internal proponents of the legislation and the Privacy Commissioner to find a correct balance in the bill prior to tabling, and therefore, could have led to legislation that was better balanced.

The Anti-terrorism Act of 2015, for example, might have struck a better balance between the legitimate needs of the state and the fundamental rights of citizens. Now, the current government has to redo it to make it balanced and satisfactory.

● (1110)

[*Translation*]

It is therefore my conclusion that in light of the increasing collection, use and sharing of personal information, the Privacy Act must be modernized so that its scope and effect are consistent with the realities of risk and the need for protection.

I will be pleased to answer any questions the committee members may have about all this, Mr. Chair.

The Vice-Chair (Mr. Joël Lightbound (Louis-Hébert, Lib.)): Thank you for your very clear remarks, Ms. Bernier.

I will now ask Ms. McCulloch of Shared Services Canada to take the floor.

[*English*]

Ms. Monique McCulloch (Director, Access to Information and Privacy, Shared Services Canada): Good morning.

Thank you very much, Mr. Chair and members of the committee, for the invitation to describe the framework that Shared Services Canada has put in place to comply with the Privacy Act. We are pleased to be joining you this morning.

My name is Monique McCulloch. I am the director of the access to information and privacy protection division, which is within the corporate services branch at Shared Services Canada. I act as the coordinator for the whole department, and I am responsible for administering all ATIP legislative and policy obligations.

I would like to add that I am also here on behalf of Violaine Sauvé, who is Shared Services Canada's chief privacy officer.

Before describing the ATIP framework, I would like to provide some context on the mandate of Shared Services Canada.

[*Translation*]

Shared Services Canada was created to modernize information technology infrastructure services so as to ensure a secure and reliable platform for the delivery of digital services to Canadians. The department aims to deliver one email system, consolidated data centres, reliable and secure telecommunications networks, and 24/7/365 protection against cyber threats

[*English*]

Shared Services Canada currently provides information technology infrastructure services across 43 departments, 50 networks, 485 data centres, and 23,000 servers.

For fiscal year 2015-16, while still growing its capacity, the ATIP office employed four full-time employees, as well as two part-time employees—one casual and one student—to carry out Privacy Act business. Shared Services Canada spent just over $411,000 to administer the Privacy Act portion of the ATIP program.

[*Translation*]

Since its creation in August 2011, Shared Services Canada has put in place a framework, anchored by internal policies, instructions and training, that identifies the procedures and processes for handling requests for personal information as well as all policy matters under the Privacy Act

[*English*]

The ATIP division introduced an ATIP management framework, which sets out a comprehensive governance and accountability structure. A total of 14 ATIP policy instruments have been established within Shared Services Canada, including a directive on conducting privacy impact assessments, as well as a standard on how to manage privacy breaches. These reflect Shared Services Canada's responsibilities under both the Access to Information Act and the Privacy Act with respect to access rights, and with regard to the collection, use, disclosure, retention, and disposal of personal information.

The ATIP division is responsible for developing, coordinating, implementing, and monitoring compliance, with effective ATIP-related policies, guidelines, systems, and procedures across Shared Services Canada. This enables the department to meet the requirements and to fulfill its obligations under the Access to Information Act and the Privacy Act.

[*Translation*]

In terms of the volume of requests for personal information, I would now like to share some statistics from the fiscal year 2015-2016 annual report on the Privacy Act.

In all, there were 123 formal requests for records under the Privacy Act, of which 120 were completed before the end of the reporting period. All 120 requests were completed within the prescribed time limits, and no complaints were filed.

[*English*]

The Shared Services Canada ATIP division weekly tracks its turnaround times in processing requests, and monitors the time limits of their completion. Performance reports are communicated to senior management each month.

In 2013, Shared Services Canada was also part of the initial ATIP online pilot project, led by the Department of Citizenship and Immigration and the Treasury Board Secretariat, to facilitate and expedite Canadians' rights of access. Today, the majority of ATIP requests received by the departments are made online as part of open government initiatives.

● (1115)

[*Translation*]

Mr. Chair, I will end here, and will now answer the committee members' questions.

The Vice-Chair (Mr. Joël Lightbound): Thank you very much, Ms. McCulloch.

I will now give the floor to Mr. Guénette and Ms. Juneau, who represent the Canada Revenue Agency. You have 10 minutes.

Mr. Maxime Guénette (Assistant Commissioner and Chief Privacy Officer, Public Affairs Branch, Canada Revenue Agency): Thank you, Mr. Chair and committee members.

My name is Maxime Guénette. I'm the Assistant Commissioner of the Public Affairs Branch, and Chief Privacy Officer of the Canada Revenue Agency.

With me today is Marie-Claude Juneau, Director of the Access to Information and Privacy Directorate at the Agency, whom you may remember from her appearance before this committee earlier this year in the context of its study of the Access to Information Act.

We are both pleased to appear before you today in support of your study of the reform of the Privacy Act.

With some 40,000 employees, the Agency is one of the Government of Canada's largest institutions. Very few organizations interact with Canadians as much as we do. In 2014-2015 alone, 31 million individuals and corporate taxpayers interacted with the CRA.

As a result, we have one of the largest personal information holdings in the Government of Canada, as acknowledged by the Privacy Commissioner. Therefore, the Agency takes its obligations under the Privacy Act and related policy instruments very seriously.

This is because the trust Canadians place in the Agency to protect their information is the cornerstone of Canada's system of voluntary self-assessment. In particular, section 241 of the Income Tax Act and section 295 of the Excise Tax Act prohibit the disclosure of taxpayer information by any employee of the Canada Revenue Agency, unless specifically authorized under these Acts. Breach of these provisions is a criminal offence and is subject to strong penalties, up to and including imprisonment.

Accordingly, recognizing the critical importance of sound privacy management, and in keeping with the recommendation of the Privacy Commissioner, the Canada Revenue Agency appointed its first Chief Privacy Officer in 2013, and I have the privilege of having been appointed to this role in two months ago, in August 2016.

[*English*]

As the chief privacy officer, I oversee all privacy management activities within the agency. This oversight is informed by ongoing performance measurement in key areas, including information technology, security, communications, and training.

As part of my duties, I am accountable for the provision of oversight, advice, and support to achieve compliance with legislative and policy requirements. In my capacity as chief privacy officer, I am required to brief the agency's management committee and our board of management on the state of privacy management at least twice yearly. I also chair a senior-level committee that addresses privacy issues as an integral part of the agency's business.

Over the past several years the agency has implemented numerous technological changes to further strengthen privacy management. We have enhanced front-end controls to our systems to ensure that employees have access only to the CRA computer systems that they require to perform their duties. We have also strengthened back-end controls to build on our automated systems for better monitoring of transactions performed by employees. These monitoring controls will be fully implemented next year, and these are as a result of a recommendation from the Privacy Commissioner in the audit from 2013.

Through a phased approach, the agency, so far, has implemented six of the nine recommendations stemming from the Privacy Commissioner's 2013 audit. Three of the recommendations involving multi-year investments continue to be implemented. We expect they'll be implemented in 2017.

Overall, the CRA has invested over $10 million and is planning further significant investment to enhance its identity and access management controls to improve the protection and confidentiality of taxpayer information and to reduce the risk of internal fraud.

We have also improved our procedures to address and manage privacy breaches so as to ensure more timely reporting of material privacy breach incidents to the Office of the Privacy Commissioner and to the Treasury Board Secretariat.

As you know, Canadians are technologically savvy and are avid consumers of online content. This makes them very sophisticated clients. They rightly expect from their government institutions the same high-quality and timely online interactions as they have become accustomed to receiving from service providers, such as Google or Amazon. For instance, we expect more than 86% of Canadians will file their taxes online next year. We expect that number to probably reach about 90% within three years.

The agency is continuing to invest in ways to improve our services to Canadians, largely through ongoing investments in IT-based solutions, such as My Account, Manage Online Mail, and MyCRA app. Yet as we work to keep pace with the latest innovations and with consumer expectations for faster, more user-centric, and more seamless service, we must ensure that appropriate measures are in place to safeguard the personal information we collect as part of our work.

● (1120)

The CRA assesses its new and modified technological advancements, programs, and activities from a privacy perspective by conducting privacy impact assessments, or PIAs. So far this year we have completed 16 PIAs, and we are on track to complete approximately 18 more by the end of the fiscal year. Our PIA plan includes 20 active PIAs at this time. This is one way we balance this fine line between meeting the expectations of Canadians with regard to service improvement, while ensuring new initiatives comply with privacy requirements.

[*Translation*]

The Agency also strives to ensure that its employees are well aware of their responsibilities in safeguarding the personal information within their custody. Our Code of Integrity and Professional Conduct, and our Integrity Framework, have been important tools to impart on employees the extent to which the protection of the privacy rights of taxpayers is central to their responsibilities, even after they leave the Agency.

Despite these measures and the many efforts to safeguard personal information, breaches do, unfortunately, occur from time to time. The CRA is keenly aware that, due to the nature of the information holdings we have, a breach of personal information can be seriously injurious to an individual or an organization. For this reason, all privacy breach incidents are assessed with a very high level of rigour. There is always room for improvement, and the Agency is continuously looking for ways to enhance its privacy management practices through program, policy and technological changes.

In fact, we regularly consult with the Office of the Privacy Commissioner and the Treasury Board Secretariat on the subject. The Agency has strong processes, policies and procedures to ensure compliance with the Privacy Act and its related policy instruments. Controls are in place, and we continue to assess and improve those controls on an ongoing basis. Our responsibility to protect Canadians' information is fundamental to who we are and what we do. That is why we continue to dedicate significant efforts to meeting the expectations of Canadians in this regard.

I hope that I've given committee members a useful overview of the Canada Revenue Agency's operating environment as it relates to the Privacy Act.

Ms. Juneau and I will be very pleased to answer your questions.

Thank you.

[*English*]

Thank you, Mr. Chair.

[*Translation*]

The Vice-Chair (Mr. Joël Lightbound): Thank you very much, Mr. Guénette.

We will now commence the first series of questions, which will be seven minutes in duration.

Without further ado, let's start with Mr. Long.

[*English*]

Mr. Wayne Long (Saint John—Rothesay, Lib.): Thank you, Mr. Chair, and thank you to our presenters this morning. It's a very interesting subject.

Ms. Bernier, I'm going to ask you a few questions. There was an article on the CBC news website that you were quoted in, entitled "Chantal Bernier says Ottawa snooping on social media". It goes on to talk about how you raised alarms—or flags, if you will—about the government collecting too much data on social media, and about the notion that if you post on social media—and I'm very active on social media through Facebook and Twitter—that's fair game for everybody. In the article you said you were seeing evidence of that from government. To quote the article:

> Bernier's office revealed that various government agencies have made almost 1.2 million requests for personal information about Canadians from Canada's major telecom companies....

That is a bit of an aside.

I want you to give us your thoughts on that, and also comment on the Cindy Blackstock case. I'd like to get your thoughts and some background on that case. How is it pertinent? What are your viewpoints?

Ms. Chantal Bernier: It's all relevant. This is exactly where I will have an opportunity to show you how the act is ill-fitting at times.

Mr. Wayne Long: That's what we want.

Ms. Chantal Bernier: Let me start with the Cindy Blackstock case, because when I was preparing my remarks, I debated as to whether I would use the PIA—the privacy impact assessment—from the RCMP, or the Cindy Blackstock case. For this, I chose the RCMP, which had a positive result. The RCMP was extremely good and well understood, but it was important for us to arc back to the charter.

With Cindy Blackstock, this is what occurred. Two departments—the Department of Aboriginal Affairs, as it then was called, and the Department of Justice—had monitored Cindy Blackstock, a first nations children's rights activist.

● (1125)

Mr. Wayne Long: Was this in 2014?

Ms. Chantal Bernier: I issued the report in 2013. It had occurred before that, so this was about two or three years ago.

Mr. Wayne Long: Okay.

Ms. Chantal Bernier: At any rate, what is very important is that she saw they were monitoring her Facebook accounts, so she came to us. We went to the departments, who said, "Well, of course. This is public. She posted it on Facebook." They were not being mischievous at all. They were acting in good faith, yet we came to the conclusion that they were violating the Privacy Act, because section 4 of the Privacy Act says that you cannot collect personal information that is not related to your activities or programs, and this was not related to their activities or programs. They replied, "But it's not personal information. She put it up on Facebook."

The crucial question at this time of technology is "What is personal information on the net?" This has been clarified in R. v. Spencer, 2014, by the Supreme Court of Canada, which ruled that personal information on the net is not public. It remains personal because personal information is any information about an identifiable individual. Hence, the posts that Ms. Blackstock was sharing with her Facebook audience were personal information that she had not intended for the government, and that the government could not justify to pick up or collect as related to its mandate—either Justice or Aboriginal Affairs—and therefore it had violated the act.

Mr. Wayne Long: I just want to jump in. You said that she became aware that they were monitoring her.

Ms. Chantal Bernier: Yes.

Mr. Wayne Long: How did she become aware of it?

Ms. Chantal Bernier: I'm searching for it. I assume that she must have had some indication. The fact that comes back to my mind is that I believe she started noticing that officials would show up at her speeches, so she connected the dots.

Mr. Wayne Long: Okay.

Ms. Chantal Bernier: She's a very highly sophisticated person. She is very well respected, intellectually very strong and very astute, so I think that she had various clues that she put together. Sure enough, indeed, that's what it was.

It really started with a lack of legal clarity as to what the obligations of the departments were, which led me, in the report of January 28, 2014, to recommend specific Treasury Board Secretariat guidelines for departments about the issue you raised, social networks.

Mr. Wayne Long: You sent a letter, I believe, to the Treasury Board president at that point, Tony Clement.

Ms. Chantal Bernier: Yes.

Mr. Wayne Long: I know there certainly were remarks in the House of Commons that the government of the day wanted to get rid of the long-form census because they thought it was intrusive, yet they were operating their monitoring of social media.

Please continue on with what happened.

Ms. Chantal Bernier: What happened is that, as far as I know, there have been no changes. I have been looking for an announcement of directives on social media. I don't know if my colleagues in the public service, who are still my colleagues, have seen anything. I certainly have seen no announcement that the government was going to comply.

But I have to tell you that the case of Cindy Blackstock was the one that we made public, but we also had years before—and it is in one of the annual reports of the Privacy Commissioner of Canada—a privacy impact assessment from a government agency where they wanted to track the social networks of public servants to make sure that they did not have illegal, prohibited political activities. While the objective is commendable—yes, it's true, I'm so proud that we have a non-political public service—you cannot monitor employees. That's personal.

In my mind, it requires further clarification to provide the departments with a clear direction.

● (1130)

[*Translation*]

The Vice-Chair (Mr. Joël Lightbound): Thank you very much, Mr. Long and Ms. Bernier.

That concludes the seven minutes available to you, Mr. Long.

I now give the floor to Ms. Rempel.

Hon. Michelle Rempel (Calgary Nose Hill, CPC): Thank you, Mr. Chair.

[*English*]

I just want to go, Ms. Bernier, back to the evidence that you presented. I just want to clarify something.

You just stated the example of the use of Facebook data, and then you compared that to the R. v. Spencer case, right? Just to clarify, I believe the ruling in the R. v. Spencer case related more to the use of IP addresses and the collection of metadata. Is that correct?

Ms. Chantal Bernier: Absolutely. They're completely different situations. In the Spencer case, what occurred is that Mr. Spencer had child pornography on his account, and that was detected. Without a warrant—this is very important, without a warrant—the police went to Shaw, his Internet service provider, to get his personal information from behind the IP address, which Shaw provided.

Hon. Michelle Rempel: Just to clarify, though, for the committee, because I was just listening to your testimony, and you were using the example of a Facebook post or putting personal information on Facebook, and then you used the example of R. v. Spencer as a rationale for why a Facebook post wouldn't be applicable. Do you still want to make that connection?

Ms. Chantal Bernier: I link them as various examples of the need to clarify the quality of personal information as "personal" on the Internet.

Hon. Michelle Rempel: Just to be perfectly clear, would you say the publication of, let's say, family activities or content of a Facebook post would be the same scope as the ruling as R. v. Spencer? I heard that linkage in your testimony and I'm not sure if that's the same thing. It was metadata, right, versus a blog post, let's say?

Ms. Chantal Bernier: Yes. First of all, in Spencer, what the court says—and this is very important—is that personal information is not what it is, it's what it reveals. It's a dynamic notion.

Hon. Michelle Rempel: To clarify, would you say that if there was a blog posted on Facebook, and then, let's say, a government department or somebody used that information, it would be in the exact same scope as the R. v. Spencer ruling?

Ms. Chantal Bernier: I would say that if the blog post, the Facebook post, is not meant for the government and the government cannot justify that it has picked it up for a valid public interest related to its mandate, that is a violation of the act.

Hon. Michelle Rempel: Is that your opinion, or can you point to relevant case law that shows that?

Ms. Chantal Bernier: Well, I would point to the findings that I made in regard to Cindy Blackstock. That was exactly the finding. We said, "Listen, Government of Canada, Ms. Blackstock's posts were personal. You collected it, yet you cannot justify that you collected it within your programs or activities, hence you collected it in violation of the Privacy Act."

Hon. Michelle Rempel: Again, just to clarify for the committee here so it's reflected in our report, R. v. Spencer would not be relevant materially in the example you gave before.

Ms. Chantal Bernier: To me, R. v. Spencer is crucial because it determines what the test is for personal information on the Internet. The test is not what the information is but what it reveals. Hence, if all you have is, say, an IP address, it's not the phone book. You cannot take it in a static form and say it's just a little number. That equates to my saying, "Please give me the key to your house", and you say, "No", and I say, "Why not? It's just a little piece of metal." It's a piece of metal that lets me go into your house.

Hon. Michelle Rempel: As legislators, you can understand that there's probably some confusion. I agree with you that there's a difference between consent in terms of...and I think a larger question is what we do with big data writ large. I certainly wouldn't want my debit card activities or my Google search results to be informative. I think even companies using that is an interesting policy discussion.

However, to me, putting something on a Facebook post with public settings is akin to pasting something on a telephone pole. At what point, as legislators, do we have to remove the nature of consent in terms of putting information into the public domain from privacy concerns? By putting information out in the public domain, isn't there an acknowledgement that you're consenting to do that? As such, the information would be considered public.

If I put a big statement about my weekend activities out in a paper format and posted it outside here, I would assume somebody would use that. I'm not sure how an electronic format changes that.

● (1135)

Ms. Chantal Bernier: The point is that the government cannot use that, because the government cannot use your personal information unless it demonstrates necessity. That's the charter test.

Hon. Michelle Rempel: That's interesting, so the test is necessity.

Ms. Chantal Bernier: Exactly.

Hon. Michelle Rempel: It's not necessarily the production of your information into the public domain. It still could be used. It's not off the table. It just has to meet that legal test.

Ms. Chantal Bernier: Necessity is crucially the test. It is articulated in section 1 of the charter. Specifically it says, “demonstrably justified in a free and democratic society”. That has been interpreted in the Oakes decision, with which you're probably familiar, as really based on four criteria: necessity; proportionality of the intrusion to that necessity; effectiveness of that intrusion, in that you have to prove that it actually works; and the absence of a less intrusive alternative. That is truly the key.

Hon. Michelle Rempel: Thank you.

Do I have any time left?

The Vice-Chair (Mr. Joël Lightbound): Unfortunately, no, but we'll be back to you perhaps later if we have some time.

Our next round of questioning will be from Mr. Dusseault.

[*Translation*]

Mr. Pierre-Luc Dusseault (Sherbrooke, NDP): Thank you, Mr. Chair.

I would also like to thank the witnesses who are before us today.

I'm pleased to see you again, Ms. Bernier.

My first questions will be about the Commissioner's fifth recommendation, namely, to expand judicial recourse and remedies. I am thinking, in particular, about the part of the last sentence which asks "that the Court be able to award a full array of remedies including damages", something that is not presently the case.

What do you think of this recommendation, Ms. Bernier? Is it possible for a court of justice to award damages against a government institution that has violated a citizen's rights, with potential financial repercussions for the citizen?

Ms. Chantal Bernier: Yes, it is.

You might be aware that the Commissioner revised this recommendation in a subsequent letter in September. He corrected or revised his sixth recommendation, which is about his role as ombudsman. In revising that sixth recommendation, he stated that Recommendation 5, to which you refer, would no longer be necessary.

That said, let's go back to the starting assumption, which forms the basis of your excellent question. There are precedents on the subject. For example, in Europe, privacy commissioners have the power to impose fines. There is therefore a monetary amount, even for government institutions that violate privacy.

Mr. Pierre-Luc Dusseault: Understood.

Mr. Guénette and Ms. Juneau, this morning, while reading the privacy policies for the My Account online program, I noted that section 9 contains the following wording:

> The CRA has taken all reasonable steps to ensure the security of this Web site. We have used sophisticated encryption technology and incorporated other procedures to protect your personal information at all times.

However, there's a small sentence that really surprised me. It reads:

> However, the Internet is a public network and there is the remote possibility of data security violations. In the event of such occurrences, the CRA is not responsible for any damages you may experience as a result.

Based on this sentence, I have a feeling you would not agree with the Commissioner's recommendation to allow citizens to be granted damages if their privacy has been violated due to the Canada Revenue Agency's My Account program.

Is that correct?

● (1140)

Mr. Maxime Guénette: I probably wouldn't go as far as saying we'd disagree with the Commissioner. I think the current statutory framework doesn't provide for anything in the nature of requiring a government body to pay damages. Naturally, if the statutory framework undergoes changes, the wording on the site might have to be changed to reflect the new framework.

To come back to the fact that there is a risk, we have, of course, adopted encryption measures. The risk exists when there is a transfer of information between the taxpayer and the Agency. Although there is encryption, there is a risk, however minimal. We try to minimize it when data is transferred. That's what we're referring to.

Mr. Pierre-Luc Dusseault: In short, if the information of millions of taxpayers who use the service were in the hands of an unauthorized, malicious person because the My Account program is not secure, there is no measure for compensating citizens whose data has been stolen?

Mr. Maxime Guénette: That's my understanding.

Mrs. Marie-Claude Juneau (Director, Access to Information and Privacy, Canada Revenue Agency): Indeed, there are no measures of that kind at this time. There is nothing to that effect in the Privacy Act.

If we lost information, or if information were compromised, we would act in accordance with the current statute. If the recommendations on the subject suggest something different, we would have to see how the Agency would react in such a situation.

Mr. Pierre-Luc Dusseault: Thank you.

I'm going to broach another subject.

The Privacy Commissioner also recommended that the coverage of the Privacy Act be extended to other federal government institutions—ideally, to all of them. It is proposed that thePMO and ministers' offices be included within the ambit of the Act as well.

At our last meeting, we heard representatives from British Columbia, Nova Scotia, and Newfoundland and Labrador. I asked them whether their ministers' offices and their premier's office are subject to the Act, and to my great surprise, all three of them answered yes. I wonder whether this is ideal and feasible. Ms. Bernier will be able to answer this question.

Upon visiting several government Web sites, including the PMO Web site, citizens are asked to provide their email address so they can receive government updates. It's nothing partisan, but data collection is involved. Would it be appropriate to make this subject to the Privacy Act?

Ms. Chantal Bernier: Definitely, and for several reasons.

First, there is currently a legal vacuum with respect to this type of personal information held by politicians' offices and political parties.

I've read this committee's previous studies. You discussed the question of whether political parties should be subject to the Privacy Act. I won't get into that, because it's not the subject of your question.

To answer your question, I would say that it would fill in a legal gap if ministers' offices were made subject to the Act. When a party is in power, it becomes the manager of the state, and exercises state powers. It should therefore be accountable for compliance with fundamental rights and for the constitutionality of state action.

If the Privacy Act were extended to ministers' offices and the Prime Minister's office, it would, indeed, be a positive development.

The Vice-Chair (Mr. Joël Lightbound): Unfortunately, Mr. Dusseault, your time is up, but we will come back to you later.

Mr. Saini, the floor is yours.

● (1145)

[*English*]

Mr. Raj Saini (Kitchener Centre, Lib.): Good morning.

The question I have is for Ms. McCulloch, and Monsieur Guénette and Madame Juneau, because you represent two institutions, and because of the amount and volume of information that you contain.

Madame McCulloch, you mentioned that Shared Services covers 43 departments. Do you have any kind of written agreement in terms of the departments and in terms of the agencies? Because now that we have moved from paper records to digital records, there is always this tendency sometimes to over-collect data. How do you prevent that sharing?

Ms. Monique McCulloch: The Shared Services Canada Act was made very explicit when it relates to the Access to Information Act and the Privacy Act. Shared Services Canada is responsible for managing the IT infrastructure, so managing the shell, but the content—all of the data residing in our data centres, even the content of emails within our networks—belongs to and is still under the control of the partner organization. Shared Services Canada, for the purposes of the Access to Information Act and the Privacy Act, has no control over the data that is residing on the IT infrastructure.

However, we are fully responsible and accountable, and work very closely with the partner institution in ensuring that the necessary privacy and security controls are in place in the management of that IT infrastructure, and when managing privacy breaches. While the data might be under the control of partner organizations—in other words, they would respond to access requests, because it's their data—if there's a breach that results from some sort of unfortunate IT infrastructure incident, Shared Services Canada would work side by side with the partner organizations to ensure that the breach is contained and managed, and the necessary corrective measures are in place. It's a shared responsibility.

Mr. Raj Saini: You've mentioned there are 23,000 servers across Shared Services Canada. If one person worked in a department or agency, would they have access? Would they have complete access to that information, irrespective of whether it was relevant to their department or agency?

Ms. Monique McCulloch: No. The partner organizations only have access to the data that is part of their mandated program activities, which is the personal information, as well as all government information holdings that are specific to their departmental program activities.

Canada Revenue Agency, for example, would not have access to the personal data of the Canada student loans program, which is managed by another federal government institution. It's siloed from that perspective.

Mr. Raj Saini: Okay.

Mr. Maxime Guénette: Mr. Chair, if I may add, in response to the question, specifically for the Canada Revenue Agency, the controls go even further than that. Twice a year, we do have a mechanism whereby we assess our employees' access to relevant applications and portions of the service. Even for Shared Services employees, they're covered by that and have been since the creation of SSC in 2011. They've complied with this ever since.

We do, twice a year, assess whether the job functions have changed, and whether some SSC employees no longer require access to specific servers or databases. That's adjusted on a real-time basis.

Mr. Raj Saini: You're such an important organization here in Canada, and you must get foreign requests for information. Once that information leaves Canada, how do we prevent that information from being disseminated or divulged in another jurisdiction where we don't necessarily have control? Do you have written sharing agreements with other countries, and how enforceable or how relevant are they?

Mr. Maxime Guénette: There are two parts to that question. We do have about 350 information sharing agreements. About 160 of these are with 46 federal organizations, and those are information agreements to share information across departments, and 186 are with provincial or territorial departments. There are some clearly established provisions in these information sharing agreements that outline the purposes for which the information is being shared and the acceptable use.

As to the extent to which these agreements are enforceable legally, my understanding is that these agreements have more of an MOU-type of reach, if you will. I would hesitate to go further on that, unless Madam Bernier has views on the enforceability of these types of information sharing agreements.

● (1150)

Ms. Chantal Bernier: Yes, I can certainly complete that in the sense that there are laws about how information can go from one country to another. The tax laws, as you know, are fundamentally international because there are agreements between countries to ensure that tax is recovered. Those are usually reflected in law, with FATCA being the most recent and most publicized example.

It's definitely enforceable. It's definitely accompanied by restrictions, and those restrictions stem from privacy law. In other words, would the federal government send tax information, through a request from, let's say, the French government? It is all subject to the privacy laws here and the privacy laws in France.

The Vice-Chair (Mr. Joël Lightbound): Okay.

Mr. Raj Saini: I'll use the 30 seconds. I have one question for you, Madam Bernier.

In PIPEDA, or when you have the difference between the private and public model, you have informed consent where you opt in and opt out. Do you think that is something we should investigate on the public side, also? In 30 seconds or less....

Ms. Chantal Bernier: No. It goes back to my answer to Ms. Rempel. The pivotal notion of legitimacy in the public sector is necessity. The pivotal notion of legitimacy in the private sector is consent.

[*Translation*]

The Vice-Chair (Mr. Joël Lightbound): Thank you very much.

It's time for the second round of questions. This time, the maximum duration will be five minutes.

Mr. Kelly, you have the floor.

[*English*]

Mr. Pat Kelly (Calgary Rocky Ridge, CPC): Thank you, Mr. Chair.

With Shared Services, I was a little surprised at the low number of requests that the department received, 123 under the Privacy Act, of which 120 were completed before the end of the reporting period. It's not clear to me exactly how long that really is, but it sounds like it's at least within the length of time in which you're expected to complete them.

During our study of access to information, we heard from both your department and other departments—perhaps we didn't hear from yours—that received access requests. We heard repeatedly that compliance was a problem with the resources available, and that backlogs, when they happened, were the result of insufficient resources and other system problems, which we've tried to address through improvements.

Why do you think you have so few requests under the Privacy Act? The first and most obvious thing that occurred to me was whether anybody knows and understands your department and the enormous volume of information handled there. I don't think I had ever heard of Shared Services until I became a member of Parliament. Are there people out there who don't know they ought to be making requests to your department?

Ms. Monique McCulloch: It connects nicely with my response to the previous question.

It was made very explicit in the Shared Services Canada Act that, for the purpose of exercising rights of access under both the Access to Information Act and the Privacy Act, the data that resides within SSC's IT infrastructure, whether it's the data centres, the email solutions, the networks, is not under the control of Shared Services Canada, but in fact under the control of partner organizations. The access requests, under both acts, must be filed by the government institution that has the mandated program activity, and therefore, overall responsibility for managing that information and making it available.

Shared Services Canada does not have a high volume of requests under the Privacy Act, contrary, for example, to the Revenue Agency or Immigration Canada or ESDC, and other government departments. Their primary bread and butter is the handling of personal information in the delivery of programs and services, such as taxpayer administration and employment insurance, but Shared Services Canada does not deliver program activities of that volume where we handle person information.

We'll have some personal information in terms of email authentication, IP addresses, that type of administration, but we don't administer federal program activities that hold known—

● (1155)

Mr. Pat Kelly: Understood, but you are the conduit through which 43 departments, 50 networks, 485 data centres, and 23,000 servers operate.

Many Canadians have concerns about privacy. There are many different ways with which Canadians may be concerned about their privacy, from the careless use by an individual in a department, to cyber-attacks and threats, or errors or negligence, or any of the things that could happen among all of these different networks and servers.

Of the requests that were made to you, are there issues of people being concerned about unreported data loss or that kind of thing?

Ms. Monique McCulloch: The majority of the Privacy Act requests we receive pertain to human resources matters. It's employees or former employees of Shared Services Canada who are looking for their information.

I think the government, through various means, has made it known that Shared Service Canada manages the IT infrastructure, but that the control of the data for the purpose of individuals to exercise rights of access.... The online tool, for example, makes it very clear that individuals have to direct their requests under both the Access to Information Act and the Privacy Act to the government organization that is responsible for administering that program.

We do receive a certain number of what we call misdirects, but our numbers are not that high on the Privacy Act side. You're absolutely correct.

[*Translation*]

The Vice-Chair (Mr. Joël Lightbound): Thank you very much.

[*English*]

Mr. Pat Kelly: That's it? Okay.

[*Translation*]

The Vice-Chair (Mr. Joël Lightbound): It is now Mr. Bratina's turn.

[*English*]

Mr. Bob Bratina (Hamilton East—Stoney Creek, Lib.): Thank you.

I was distracted earlier on from some of the testimony, because an old acquaintance, an architect who works on projects around the world, replied to my request to his email, "It's phishing. Get rid of it." I had to change my password.

In light of that, Ms. Bernier, the technology is constantly evolving. You're part of a really huge organization. It's governmental in size, I would say.

Ms. Chantal Bernier: It's the biggest law firm in the world.

Mr. Bob Bratina: Are you able to compare the kind of security that your firm has to provide with what you know of the Canadian government?

Ms. Chantal Bernier: I would say that we have to be even more careful, and we are even more careful, first of all because our information is solicitor-client privileged. It is therefore protected not only as personal information but also by the duty of confidentiality towards our clients.

Secondly, because we are worldwide, we have to make sure that we have worldwide protection. At the same time, the advantage of being worldwide is that we have the same footprint as our clients. Our clients love the fact that they can come to just me, yet I can connect to the whole world to respond to their issues as they occur in the whole world. We therefore need interoperability and that interoperability must be secure.

Obviously we pride ourselves on having that extremely secure environment that is governed by a very sophisticated governance architecture, as you will imagine, that allows us to be truly well coordinated and yet completely secure.

● (1200)

Mr. Bob Bratina: Why shouldn't we be able to provide the same level of confidence to the people who deal with the government?

Ms. Chantal Bernier: Having investigated government organizations for six years, I do have quite a bit of sympathy. In fact it's interesting, because the audit that Mr. Guénette was referring to is an audit that I actually supervised. While we made recommendations for improvements, we were very much aware of their challenges.

There are 400,000 employees, do I have that right?

Mr. Maxime Guénette: No, it's 40,000.

Ms. Chantal Bernier: You see? In my empathy I made the number bigger.

Voices: Oh, oh!

Ms. Chantal Bernier: There are 40,000 employees of various levels who need to reply to people who call from everywhere, as Monsieur Dusseault was saying. They need to reply, so they need to have access to the files, yet it has to be controlled. It can't go out. It's sensitive information. That's the first complexity, that it's operational, with so many people at so many levels.

The second complexity is that the government does want to have access to some of the information. For example, we know that "follow the money" is key to uncovering illegal activities. That means there has to be some authorized access in spite of all the protections. That's another complexity.

Then, with 400,000 people in the public service—this number is correct—that's a lot of people to monitor. That's a lot of people who could have a grudge, who could have some malicious intent. I've seen lots of them. I haven't seen them only in government. I've seen them in the private sector as well. If you look at the internal threats to data security and the external threats to data security, you realize that the risk is very high.

One advantage we have in our law firm, since you made the comparison, is that we're all lawyers. We are all lawyers who have a vested interest in this business flourishing, and therefore we have a culture that favours, that helps, data security. In the government, however, you can have a disgruntled employee. You don't have an employee who at the same time has a personal investment of money in the business. You have different contingencies to contend with.

I can tell you about one agency for which I have a lot of sympathy. It was also very operational. Their main challenge was their disengaged staff. Because the staff was disengaged, the staff did not exercise the proper discipline that they should have.

Mr. Bob Bratina: Is there more time?

The Vice-Chair (Mr. Joël Lightbound): No. We'll have some more time at the end, most likely.

We're now going back to Mr. Kelly.

Mr. Pat Kelly: Thank you, Mr. Chair.

We had quite a discussion in our previous meeting around the mandatory reporting of privacy breaches. I'll give each of you a minute to comment on what you think about thresholds and what would constitute the type of material breach that would necessitate the mandatory reporting to the commissioner and how to mitigate against additional harm to an individual that may result from the act of reportage.

Ms. Chantal Bernier: This is a case where PIPEDA is a good model to follow. I think the government got it right in PIPEDA for mandatory breach notification. That means, first, it is only notification where there is a real risk of significant harm. You don't want to alarm people for nothing.

Mr. Pat Kelly: Indeed.

Ms. Chantal Bernier: The harm could be either moral or financial. It could be to reputations or to relationships, but you need to take into account significant harm.

The obligation to notify is not specified in a specific timeline. It is as soon as possible, which I believe speaks to due diligence yet does not constrain the organization in what are technologically more defined delays than what could be specified in law. Also, the notification must go to both the affected individuals and to the Privacy Commissioner.

To go to your last point, how it helps is that when you notify individuals then you empower them to take measures to protect their personal information.

● (1205)

Mr. Pat Kelly: Ms. McCulloch.

Ms. Monique McCulloch: Sometimes, for institutions to define a material privacy breach tends to be a challenge. One institution will deem something as a material breach and another will not. I know additional standardization is an ongoing effort across the government.

Because the level of sensitivity is discretionary, you could have something that is extremely sensitive but implicates only one individual, whereas you could have something of very low sensitivity that implicates hundreds, sometimes thousands. It's left to the discretion of each institution to determine whether something is deemed to be a material privacy breach, and to therefore notify the Privacy Commissioner's office, as well as the Treasury Board.

Mr. Pat Kelly: Is there a need for more clarity?

Ms. Monique McCulloch: At times, for standardization across the government, in my view, yes. There could be some value added with more benchmarking and more criteria.

Mr. Pat Kelly: Thank you.

Mr. Maxime Guénette: Obviously, the Canada Revenue Agency takes into account the sensitivity of the information that's disclosed in assessing the severity of the breach. We have medical information, financial information, and personal identifiers like social insurance numbers. Those kinds of things would very obviously trigger the reporting of a breach, anything that could lead to the risk of identity theft or fraud.

However, to your point, and to speak a bit to what Madame McCulloch was alluding to, there are different types of breaches. One type of breach we see a lot in the CRA has to do with misdirected mail. The volume can appear to be high from an absolute number perspective, although I would flag that from a percentage point of view, given the 110 million pieces of mail that we move in a year, it is less than 0.001%. However, a piece of correspondence that went to the wrong address, wasn't opened, and was sent back to us, we log as a security breach internally. This isn't something that would warrant flagging to the Privacy Commissioner.

A security breach that has to do with an employee willfully accessing taxpayer information outside his normal duties is treated very differently. If I'm not mistaken, the 20 or 21 cases that were flagged with the Privacy Commissioner all had to do with wrongful access to taxpayer information by employees. There's quite a range, and different departments' business would very obviously be quite different. There is a certain amount of flexibility, which is built into the current framework, that's useful.

[*Translation*]

The Vice-Chair (Mr. Joël Lightbound): Thank you.

Ms. Dzerowicz, you have the floor for five minutes.

Ms. Julie Dzerowicz (Davenport, Lib.): Thank you, Mr. Chair.

[*English*]

Thank you very much for the informative presentations.

I wasn't going to ask this, but Mr. Long asked some excellent questions that triggered it. In my riding, when I go door to door and talk to people, it seems there is this belief that the government collects data around web activity and cellphones. At first I thought they were just worried about Bill C-51 and the type of data that was being collected and then moved between the RCMP and security, but I think there's a general belief out there. I can't tell you that hundreds of people have said it to me, but there is this belief.

I know that you've mentioned that government cannot use personally collected information unless it meets the necessity test, but does it actually collect that information? I just want to get a sense of whether I need to say to people, "No, you're just reading too much conspiracy-theory type stuff." Could someone answer that? I'd like to be able to honestly respond back to people.

● (1210)

Ms. Chantal Bernier: I certainly can take a first try at it.

I think there is a lot of misinformation, which is why—and I'm going back still to the report of January 28, 2014, because it focused so clearly on this—we made 10 recommendations that I really hope will not be forgotten because they address those very practical issues. One was transparency. Can the government tell us more specifically what it does?

From having been both at Public Safety Canada, where I was assistant deputy minister, and at the Office of the Privacy Commissioner, I can tell you that it's really not that bad. There is no Big Brother. The government doesn't have the money, it doesn't have the interest, and frankly, it's much more strategic and ethical than this representation.

However, the comments you hear—and I know you do because I hear them, as well—really underscore the need for greater transparency, specifically that there be annual reports for all the agencies that collect public safety information or collect signal information, and that there be regular appearances by the heads of these agencies before House of Commons committees, such as this one or public safety, etc. Bring them to account and say, "Once a year, we want a report from you. What do you see as a threat, what are your activities in relation to the threat, and how do they respect fundamental rights?"

Ms. Julie Dzerowicz: You originally started your presentation by talking about information sharing agreements between states and agencies. Who does it well? Which country does it well? Do the agreements that end up being created identify how long the data is kept? If there are errors in data that's being sent over, if there's some misinformation that goes from Canada to Austria, and then all of a sudden we correct it, is there some sort of mechanism to do that on the other side, as well? To what extent do we actually inform? If a person's data is being transported, to what extent do we inform the person that their data has been shared with other states and agencies?

Ms. Chantal Bernier: Nobody does it ideally. The remedies you referred to are very fragmented. For example, the passenger protect program does have a remedy whereby if you are stopped because of the no-board list—we've all heard about the seven-year-old boy who was denied boarding because he happened to have the same name as someone who's on the list—there is a remedy process. It takes a very long time, but Minister Goodale has already announced that they're looking at addressing that. In fact, it is part of the green paper "Our Security, Our Rights" that is being put to consultation.

My answer to you is that, sadly, I cannot answer because the level of transparency that would be needed to know the answer to your question is simply not there. Every country must step up.

Ms. Julie Dzerowicz: How much time do I have left?

The Vice-Chair (Mr. Joël Lightbound): None—

[*Translation*]

Ms. Julie Dzerowicz: Okay.

Thank you.

[*English*]

The Vice-Chair (Mr. Joël Lightbound): —but we'll have some more time at the end.

[*Translation*]

Mr. Dusseault, the floor is yours, and you have three minutes.

Mr. Pierre-Luc Dusseault: Thank you, Mr. Chair.

My question is for the Canada Revenue Agency representatives, and is about the measures taken in the event of privacy violations.

Recently, a USB key or a laptop—I can't remember which—was left in a bus. Malicious people got access to CRA data. The vulnerability that made this possible is called Heartbleed.

In another incident, the CBC made an access to information request, and was given a file mistakenly in response. So the CBC ended up with very sensitive information, and, naturally, it reported on all that information.

I'd like to know exactly what measures are being taken in this regard. Earlier, there was talk of possible damages, but you don't seem to be envisaging them for the moment, since they're not mandatory. What do you do to inform and reassure taxpayers in such cases? Do you take measures to attenuate the repercussions for the victims of these privacy breaches, such as ensuring that their credit score remains good? When the data falls into the wrong hands, what do you do? How do you react?

● (1215)

Mr. Maxime Guénette: Since this was something that happened at a very high level, I'm going to ask Ms. Juneau to explain the details of the relevant procedure.

There is indeed a procedure within the Agency. We work with the Agency's security officer, who is our first point of contact. Incidents must be reported to that person, and that person must prepare a report.

A bit earlier, we spoke about the criteria we use to assess how serious the breach is. Ms. Juneau is consulted to determine whether there has been a breach of privacy, and if there has been, the measures to be taken are discussed. If the risk evaluation matrix provides for it, we contact the taxpayer. That's part of the steps to be taken.

Ms. Juneau, would you like to add something on the subject?

Mrs. Marie-Claude Juneau: Yes, certainly.

As Mr. Guénette just mentioned, the Agency follows a well-established process for reporting all types of incidents. Following an incident, the Security and Internal Affairs Directorate conducts an investigation and sends us its findings. The question to be determined is whether there's been a security breach. If there has been we report the breach to the Privacy Commissioner. We also have a disciplinary framework at the Agency. Based on that framework, we verify how the breach was reported, and whether a disciplinary measure is applicable in such a case.

As for what we do to mitigate the impact of security breaches, I will come back to the example you gave concerning the CBC. When the incident occurred, what we did in terms of access to information and privacy measures was to verify the processes implemented by the Agency, and determine where surveillance or review could be enhanced with a view to preventing such a situation from recurring.

Another process was developed too. A private firm verified whether our processes were indeed adequate, and whether there were still shortcomings. Following that audit, the firm made a few recommendations. The measures it recommended were mainly about systems, system audits, and quality assurance. We have implemented those procedures, to prevent such situations from recurring.

Mr. Pierre-Luc Dusseault: Thank you.

Actually, you have already answered my second question, about the procedures put in place to ensure these types of incidents don't happen again.

In any event, I think the time available to me has elapsed.

The Vice-Chair (Mr. Joël Lightbound): It has indeed.

However, we've finished the official question period, and we're ahead of schedule. So I extend an invitation to those who have questions, but have not yet intervened. I can already see that Mr. Massé would like to intervene; as for Mr. Dusseault, if you have additional questions, you'll be able to ask them a bit later. The same suggestion applies to Ms. Rempel and Ms. Kelly. Just give us a hand gesture if you have any other questions.

Mr. Massé, you have the floor.

Mr. Rémi Massé (Avignon—La Mitis—Matane—Matapédia, Lib.): Thank you, Mr. Chair.

I thank the witnesses for taking part in this meeting of the committee. It's much appreciated.

My question is for Mr. Guénette.

As far back as 2013, the Privacy Commissioner had conducted an audit, and pointed out the deficient CRA security practices. He also said that, because of these suboptimal practices, the CRA had made it easier for employees to improperly access thousands of documents over the course of several years.

You've made reference to these 2013 recommendations. Tell us about the measures you put in place to ensure this type of situation no longer occurs.

● (1220)

Mr. Maxime Guénette: Thank you very much for the question.

Mr. Chair, two types of actions were taken in that regard. One is more technical, and the other is about employee education.

From the technical standpoint, we're continuing to implement measures. In fact, I alluded to them in my preliminary remarks. They have been and are continuing to be put in place, in order to better document and control employee access to Agency databases and applications. As I was mentioning, reviews are done twice a year, to ensure that if there are changes to the duties of certain employees, and access needs to be reviewed, it's done.

Improvements were also made so that an "audit trail" can be created in the National Audit Trail System. This makes it possible to detect accesses not tied to certain duties, and to notify managers of those accesses. So measures were put in place so that managers can receive automatic notifications of this kind. For example, I might need to speak to Ms. Juneau because I received an indication that she accessed some information that doesn't seem to fit with her duties. Several applications are subject to this type of audit.

Mr. Rémi Massé: Are they in operation now?

Mr. Maxime Guénette: Yes, they're in operation, but they continue to be improved. We anticipate the work will be finished in 2017—that is, by the end of next year. Those are the more technical elements.

However, since that 2009 audit, a lot of emphasis has been placed on employee education. We have certain data that enables us to identify the cases where privacy breaches are reported the most. This is because, as you were saying, what needs to be reported is now clear to employees, compared to the situation five years ago. There's the Integrity Code, to which I've referred. There's also the Integrity Framework. Added to that are the communication initiatives we've implemented, and mandatory training. There are several indicators on our performance management dashboard. As Chief of Privacy, I must check on the extent to which employees are doing training, and the extent to which they're consulting the available information. For example, we recently made a video available. Based on the most recent numbers we have, it was viewed more than 12,000 times by employees. The video explains the kinds of privacy breaches that can occur inadvertently.

All this to say that a major communications effort has been made in this regard, and certainly must continue. We see—and I think the data support this—that there is now a better understanding of the importance of protecting personal information, of what can constitute a privacy breach, and of the procedure to follow so these breaches can be identified when they arise.

Mr. Rémi Massé: Do I still have 30 seconds?

The Vice-Chair (Mr. Joël Lightbound): Yes. You have 30 seconds.

Mr. Rémi Massé: Ms. Bernier, if I understand correctly, you helped develop this audit process. Did you have a chance, subsequently, to verify the measures put in place by the Canada Revenue Agency? Mr. Guénette provided some explanations about these measures. Based on what you've seen, it is your impression that the measures put in place are sufficient? Or do things have to be taken further as far as the Agency is concerned?

Ms. Chantal Bernier: Obviously, it's my successor who is now keeping track of the subject, and he is the one who can answer this question. I can only speak to the situation up until June 2014. At that time, I was very convinced that the Agency was taking our recommendations very seriously. The recommendations identified shortcomings, but these were taken seriously. I can't discuss the current situation, but when I was present, I was seeing a real effort on the Agency's part.

● (1225)

The Vice-Chair (Mr. Joël Lightbound): Thanks.

And thank you, Mr. Massé.

I now give the floor to Mr. Dusseault.

Mr. Pierre-Luc Dusseault: Thank you, Mr. Chair.

I have a few brief questions to ask.

Ms. Bernier, I would like to go back to what you said about political parties, which you didn't have time to expand on.

I asked the same question to the British Columbia representative this week. He told me that the political parties in that province, including both the provincial and municipal levels, were covered by the act, but I would like to address the legislation that applies to the private sector.

In your view, what would be the best solution to consider? Could the legislation that is applicable to the private sector technically apply to political parties? Is it conceivable to make it apply?

Ms. Chantal Bernier: The Personal Information Protection and Electronic Documents Act would have to be amended to create a separate part, because the statute applies to the private sector, and is based on the consent paradigm, as part of business activity. In other words, I give my personal information in exchange for a good or service. That is not at all what is happening when information is given to a political party.

PIPEDA should be expanded to include all non-governmental relationships. It should contain a part applicable to business activities, which is the case at present. This covers situations where personal information is imparted in a transactional context. There should be a part applicable specifically to political parties.

Mr. Pierre-Luc Dusseault: We will certainly take that into consideration as our work continues.

In the Agency's report to Parliament on the application of the Privacy Act, there is reference to a case where information was requested, but a translation from English to French was refused. There is little explanation—just a short paragraph of the report deals with this question. Moreover, in the appended tables, there is only one instance of refusal.

If you have any information on this, could you provide me further details? Why was this information not translated so the person concerned could have it in the language of their choice?

Mrs. Marie-Claude Juneau: Thank you for this very good question, but unfortunately, I don't have the answer. I will do some research and ensure the answer is sent to the committee in the coming days. I apologize.

Mr. Pierre-Luc Dusseault: Not a problem. There's no way to be familiar with the details of each of the 3,000 requests made.

Mrs. Marie-Claude Juneau: Indeed.

Mr. Pierre-Luc Dusseault: It would still be useful for the committee to obtain that information.

Mrs. Marie-Claude Juneau: Certainly.

Mr. Pierre-Luc Dusseault: I have one last question to ask, Mr. Chair.

One case concerning data management subcontracting was reported. The Privacy Commissioner investigated a matter involving Shred-it, a company that stores data, presumably in paper format. There's a large volume of paper documents at the Canada Revenue Agency, because it retains certain information for dozens of years.

Do you take additional measures in the case of a subcontractor or a private company that manages Canadian taxpayer data? Who don't you look after this internally? Why isn't it managed by your department? Why subcontract when the department could do it directly?

Mrs. Marie-Claude Juneau: I couldn't say why we subcontract rather than doing it internally. However, I can say that a process has been established so that firms—I forget the exact term but it pertains to contracts—meet our requirements, and do everything we want in terms of privacy.

You referred to the Privacy Commissioner's report. We contacted the Commissioner and we met with him a few times during this process, to explain what we were expecting from the company at the time. The complaint filed with the Privacy Commissioner was about the fact the information was managed by a company located in the United States. Ultimately, the Commissioner conducted an investigation and verified certain things. He concluded that the complaint was not well-founded.

● (1230)

Mr. Pierre-Luc Dusseault: That was the Commissioner's finding.

Who would be able to answer the question about the policy allowing for the use of subcontractors for data storage? Is this more of a policy decision?

Mr. Maxime Guénette: No, I don't think so. If I understand correctly, it's purely for operational reasons.

I'd like to clarify that all the documents are paper documents, handled by a company called Recall. I can do some checking and get back to you with a more detailed answer on the subject.

My understanding is that the Agency uses subcontracting so it can realize economies of scale. The Agency has more than 100 sites in Canada where documents can be retained. The retention of all these documents within a single organization calls for rather impressive record management technology, and the documents must be locatable in boxes using bar codes. Rather than invest in these kinds of technologies in its numerous centres, I suspect the agency uses subcontracting primarily for efficiency and economies of scale.

Mrs. Marie-Claude Juneau: Mr. Chair, may I add something on this subject?

The Vice-Chair (Mr. Joël Lightbound): Go ahead, Ms. Juneau.

Mrs. Marie-Claude Juneau: I'd like to add something to what Mr. Guénette has just said.

Before we opted to use the services of that company, the document management was done by Library and Archives Canada. It never really gave up that function. It's simply that it's not necessarily part of its new mandate. So we had to find a solution to ensure that document management continued. Prior to this, it was done internally by the government.

Mr. Pierre-Luc Dusseault: Thank you for your answer.

The Vice-Chair (Mr. Joël Lightbound): Thank you very much.

Mr. Kelly now has a few questions.

[*English*]

Mr. Pat Kelly: Thank you, Mr. Chair.

Commissioner Therrien had initially recommended something short of having order-making power, but he recently changed his recommendation to indeed ask that his office be given order-making power and go to that model of office.

I'd like, Ms. McCulloch and Mr. Guénette, for you each to comment on how you think that will impact your organizations.

Ms. Monique McCulloch: My expectation, given years of working with the commissioner's office, is that the approach will likely continue to be one of an ombudsman, as the ultimate goal for the commissioner's office, as well as the institution, is to resolve the matter as quickly as possible and to the complainant's satisfaction. I would expect that the cases where orders must be issued will be few and far between, and I don't think it will have a huge impact.

It will be handled very similarly to current situations, where, if the commissioners were previously recommending a particular resolution to a complaint, the matter would be dealt with at a very senior level of the organization. But those are limited cases, whereas the majority of matters are normally resolved at an operational level, so I don't expect a huge impact on that end.

The government will always have the opportunity to go before the court should there be a real difference of opinion from a risk perspective. If we receive an order to release records, where we feel it would have a grave invasion of privacy, or we feel there's a public interest that outweighs the invasion of privacy, the matter could be taken to the next level of review, but it should be in very limited cases.

● (1235)

Mr. Maxime Guénette: Thanks for the question.

Very similarly to Ms. McCulloch, I would think we approach our dealings with the Privacy Commissioner with the intention to find common ground, and if we enter a different legislative framework where there is an order, we would attempt to resolve the situation before it comes to that.

In terms of what that particular change might imply for our work, it's hard to speculate on what that might look like, without knowing more of the specifics of how that would roll out. Certainly with a place like CRA, with the volume that we're dealing with, depending on how this gets rolled out, there may be an impact in terms of our processes and our resources, which we would need to address, but we would comply with whatever framework is put in place by the government.

Yes, I think I would agree with Ms. McCulloch that the attempt is to find common ground, and then, for the most part, we are successful in doing that.

Mr. Pat Kelly: Do you agree with the recommendation to go to an order-making model?

Some critics in our study of access to information have argued that when you have order-making power, you cease to become an ombudsman and you become an adjudicator. Instead of being an advocate for privacy, you become a person who makes a judgment about a particular case, rather than just advocating for privacy.

Do you share those concerns, or do you believe that the order-making model is the correct way to go with privacy?

Mr. Maxime Guénette: I would hesitate to express an opinion as to whether or not that's the right way to go. I think my role with the agency would be to implement whatever decision gets made in terms of the legislation. Certainly, as I said, with or without this order power, our attempt is to comply with the letter and the spirit of the act to the extent possible, and we would do that under either framework.

[*Translation*]

The Vice-Chair (Mr. Joël Lightbound): Thank you very much, Mr. Kelly.

I now give the floor to Mr. Long.

[*English*]

Mr. Wayne Long: Thank you, Chair.

Ms. Bernier, in another article I read, you gave some comments about the anti-spam legislation. Obviously, there are businesses and marketers that think it's restrictive, and then obviously from an individual standpoint, I understand it's there to protect us from being bombarded with too much.

Can you just give me your comments? Do you think there's a balance there, or do you think the legislation is strong enough?

Ms. Chantal Bernier: First of all, I conclude that I write too much. Really.

CASL is a completely different subject, and as you know, very controversial in industry. On the other hand, the Office of the Privacy Commissioner has issued its first investigation into CASL this summer, and I believe that consumers will be happy to see the restrictions that have been put on industry.

To answer your question of whether it hits the right balance, I would suggest we wait a few more years. What I mean by that is that we should accumulate more experience on how business feels that it responds to a genuine desire for promotional ads or information and their own needs.

There is consent. You can obtain the right to get promotional information, and in fact the comparison that Mr. Saini made a moment ago about opting in and opting out, this is under the Privacy Act but is an architecture of control that can allow the sending of promotional—therefore commercial—economic messages to a consenting recipient and to make a definition that you want everything or you don't want everything. There we can find a proper balance between the rights of the consumer not to be bombarded, as you say, and the needs or the desire of the organization to help its marketing initiatives through that.

● (1240)

Mr. Wayne Long: How concerned should we be about consumer apps demanding too much permission? I don't know if it was your office, but one of the Privacy Commissioners' offices did a sweep. I think it was of 1,211 apps where 75% of them requested either location, access to ID, camera, or contacts. How concerned should we be about that?

Ms. Chantal Bernier: We should be quite concerned, but the good thing is that we are and the Office of the Privacy Commissioner survey of January 2015 showed that Canadians are not only appropriately concerned but they're actually taking action and will now, more and more, refuse to download apps that are overly intrusive. I think the awareness is now giving rise to action, and that's the way to vote. We vote with our fingers, I suppose in this case. You don't press send. You do not send them their information. You do not download.

We need to be aware of that, and we need to make sure we hold the app developers and the companies to account to minimize the information they seek through the apps, or as you were referring to a moment ago, Mr. Saini, if they do want to collect a lot of information because they want to do business intelligence, because they want to tailor their services to you, then they need to have specific consent for that.

Mr. Wayne Long: Okay, thank you.

[*Translation*]

The Vice-Chair (Mr. Joël Lightbound): We now move on to Mr. Bratina.

[*English*]

Mr. Bob Bratina: Thank you.

Ms. Bernier, I believe you said early on that you looked favourably on the recommendations. I don't know if you're able to carefully analyze the whole report, but let me ask you a specific question. In recommendation 15, the Privacy Commissioner suggests amending the act to extend coverage to all government institutions, including ministers' offices and the Prime Minister's office. What would you see in that recommendation?

Ms. Chantal Bernier: As I've mentioned to Mr. Dusseault, I see this favourably, because we have a legal void at the moment in this regard. In other words, there is personal information held or could be held in these offices that is not currently protected. When you look at the fact that the government in power, the ministers, the Prime Minister, do exercise the powers of government, they should be held to the standards of the Privacy Act to collect, use, or disclose that information.

Mr. Bob Bratina: In recommendation 11, the suggestion is amending section 64 to allow the commissioner to report publicly on government privacy issues where he considers it in the public interest to do so. The Privacy Commissioner already has the power to issue special reports and annual reports and so on. Is the expansion of this useful in your view?

Ms. Chantal Bernier: It is, absolutely. I was confronted with this when we finished the investigation of, as it was then, Employment and Social Development Canada. You will recall that it lost a hard drive of 583,000 Canadians' financial information. It was just too big, I felt, to leave it to the annual report. I thought that the Canadian public deserved a quicker result of our investigation, and therefore, proceeded by tabling a special report.

But it is quite stilted and onerous. It is demonstrating a lack of flexibility. I was wanting to serve the Canadian public well by stating the results of our investigation, but I could only do it through the special report procedure.

I believe that this recommendation is very cohesive in the transparency theme of the commissioner's recommendations.

● (1245)

Mr. Bob Bratina: How do you see it working in the case of some major breach or something? Would the Privacy Commissioner advise the government that he intended to speak to that, or just how do you see that working?

Ms. Chantal Bernier: As I mentioned when I described the status of the Privacy Commissioner as an agent of Parliament, he does not need to inform government. He just goes out and says this is what he has discovered and this is what he is reporting on. The way it is done, it would be at the end of an investigation, or it could be as we did for ESDC.

When the news came out, I immediately announced that I was initiating a complaint, because the commissioner can either initiate the complaint or reply to complaints filed by a plaintiff or many complainants. This was really too big not to do something about it, so I chose to initiate a complaint. Then I chose to publish the report outside of the annual report, but the artificiality of that constrain I had, which meant I had to do a special report, was really not justified. It really was a hindrance to transparency, for no use.

Mr. Bob Bratina: Is there anything in the review that leapt out as missing, that you thought might be addressed in the recommendations?

Ms. Chantal Bernier: The departure I would make is the one I have underlined, and that relates to the recommendation on necessity. That's recommendation 4, where the Privacy Commissioner says that it should be proven to be necessary to the program or government activity. I believe that inherent test is not sufficient. It should be an external test grounded in the charter.

Mr. Bob Bratina: Yes. Those are good comments. Thank you.

The Vice-Chair (Mr. Joël Lightbound): Thank you, Mr. Bratina.

We still have Madam Dzerowicz and Mr. Saini who would like to ask a few questions. I'd ask you to keep it relatively short because we have about 10 minutes left.

We'll start with you, Madam Dzerowicz.

Ms. Julie Dzerowicz: Thank you very much.

I know that the Privacy Act is different from PIPEDA. Google collects a lot of information on me. Should there be a better relationship between the two, PIPEDA and the Privacy Act? That's a general question.

The second thing is that technology changes fairly quickly now. How do we keep our legislation sort of agile and ongoing?

Then I have another question for Ms. McCulloch and Mr. Guénette.

Ms. Chantal Bernier: How relevant.

First of all, just to put it in perspective, Europe does not have separate legislation for private and public sectors, and I have often questioned in my mind whether we should. But we do and we have an excellent system. The reason we do is easily justified by the difference in legal paradigms that are the subset of both. This, again, goes back to my answer to Ms. Rempel, meaning one is the state-to-citizen relationship Privacy Act and that is grounded strictly in necessity. The state cannot intrude upon your privacy unless it is demonstrably justified in a free and democratic society.

The relationship you have with other data holders, say Google, Facebook, or any company you buy something from, is predicated on your relationship, your free relationship with them, and therefore is built on consent.

I think that the way we have it constructed is working very well. However, the bridge that you're pointing to is extremely important and increasing. We've seen it with what is often referred to as the deputization of the private sector. Obviously, the big showdown of Apple and the FBI is an example of that in the U.S., where you have this treasure trove of information in the private sector that the law enforcement agencies, therefore the public sector, wants to have access to. How do we regulate that connection?

There has been clarification in Canada. One clarification was, as I mentioned earlier on, R. v. Spencer. A more recent clarification that goes more directly to your question is in R. v. Rogers Communications Partnership. That was January 2016, where the issue at hand was a judicial warrant for a tower dump, a tower dump being giving to the police all of the exchanges, communications, within the vicinity of a specific cellphone tower, which would have resulted in providing the police with 43,000 people's exchanges between, say 3:00 and 5:00 on that day. Why? Because there had been a jewellery robbery at that time on that day. Rogers said, no, opposed the warrant, and the police stood down. However, Rogers still went to court and said that warrant was invalid because it was overly broad. The police replied via the Auditor General that Rogers had no standing in fighting this issue, whereas the court—and this is very important to your question—said not only was Rogers right in refusing to comply with a judicial warrant because a judicial warrant was too broad to be constitutional, but it had the obligation to oppose the warrant as its contractual duty to its customers.

That really illustrates, I believe, the link you're making between public and private.

● (1250)

The Vice-Chair (Mr. Joël Lightbound): It will be Mr. Saini now for three minutes.

Mr. Raj Saini: I have one final question, Madam Bernier. You raised an interesting point that I found very curious. You talked about how Dentons is worldwide. Obviously if you have worldwide offices, you have different privacy regimes in different jurisdictions. Because whenever you have a regime in any country there's an application of resources whether they be human or financial, if you have clients who are doing business in multiple jurisdictions, how do you equilibrate all of that to have one standard?

Are there multiple standards, or do you devolve to the jurisdiction where the business is occurring or where the case is being tried or heard? How to you equilibrate all that?

Ms. Chantal Bernier: We have to follow the law everywhere we operate, and the law is different in different countries.

I was in our Singapore office recently and we were discussing, specifically, how you regulate privacy law in Singapore, but in that case, it was a Canadian business going there. The jurisdictional rules around privacy law are such that where the operation takes place, where the information is collected, must always correspond to the laws of the country where it is collected.

However, there are different laws for cross-border. There are countries that do not allow the cross-border transfer of personal information from their citizens, except with very tight rules, conditions, and so on. There are other countries who are mainly requiring due diligence, saying you can go cross-border but make sure that through the transfer you protect the information at the same level as, say, Canadian law requires you to. They do that by, first, choosing very trustworthy contractors, and second, by having contractual clauses that specify, the contractor will protect the information at the level they, the customer who's using the contractor to transfer the information, are held to and that they will audit and inspect the contractor. There are compliance measures like that.

Yes, it is definitely a conflict of laws challenge, but one that is governed by rules of conflicts of laws.

The Vice-Chair (Mr. Joël Lightbound): Thank you very much. I would have had some questions for Madame Bernier, but I guess we'll have to reinvite you. It was with a sense of sacrifice, as I chaired, that I didn't get to ask my questions, but some other time.

Thank you all for being with us today. It was greatly appreciated, and I want to wish all members a happy Thanksgiving. We'll see each other again in two weeks.

[*Translation*]

Thank you, everyone, and have a good day.

The meeting is adjourned.