HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

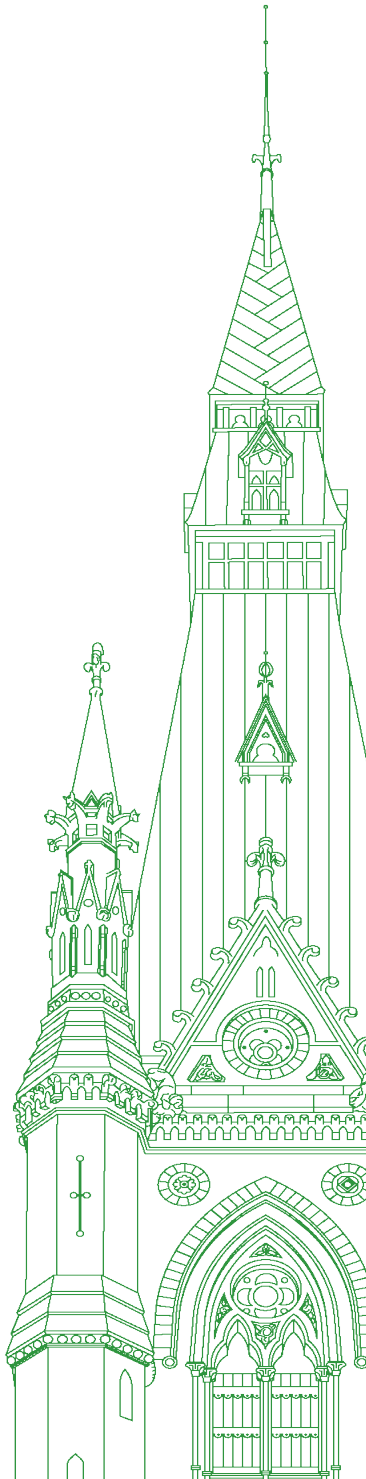
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 143

Thursday, December 5, 2024



Chair: Mr. John Brassard

Standing Committee on Access to Information, Privacy and Ethics

Thursday, December 5, 2024

● (1600)

[*Translation*]

The Chair (Mr. John Brassard (Barrie—Innisfil, CPC)): I call this meeting to order.

Welcome to meeting no. 143 of the House of Commons Standing Committee on Access to Information, Privacy and Ethics.

Pursuant to Standing Order 108(3)(h) and the motion adopted by the committee on Tuesday, October 29, 2024, the committee is resuming its study of privacy breaches at the Canada Revenue Agency.

[*English*]

I would like to welcome our witnesses today.

We have, from the Office of the Privacy Commissioner of Canada, Mr. Philippe Dufresne, who is the Privacy Commissioner, as well as Isabelle Gervais, who is the deputy commissioner, compliance.

Commissioner, I've given you up to 10 minutes to address the committee with your opening statement. Please go ahead.

Thank you.

[*Translation*]

Mr. Philippe Dufresne (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): Thank you, Mr. Chair.

Members of the committee, thank you for the invitation to speak to this critically important issue.

Data breaches have surged over the past decade, in scale, in complexity, and in severity. As stewards of sensitive personal information, government institutions are attractive targets.

To ensure that personal information is protected, federal organizations, including my office, must be continuously adapting to an evolving threat environment.

[*English*]

In February 2024, we tabled a special report to Parliament with our conclusions on an investigation into a 2020 credential stuffing incident that impacted the Canada Revenue Agency, or CRA, and Social Development Canada, or ESDC.

During the final stages of this investigation, we learned of other breaches related to CERB fraud that the CRA had not reported to the OPC, dating back to 2020 and affecting up to 15,000 individuals. We indicated these breaches in our special report and added that we would be following up on this with the CRA.

The OPC recommendations in this investigation included improving communications and decision-making frameworks to facilitate a rapid response to attacks and developing comprehensive incident response processes to prevent, detect, contain and mitigate future breaches. Both the CRA and ESDC agreed to implement these recommendations.

On May 9, 2024, the OPC received a breach report from CRA, retroactively covering incidents from May 2020 to November 2023, which captured 31,393 separate incidents. The OPC's breach response team has met regularly with the CRA since then to find out more about the CRA's response to the situation and to be kept up to date on the actions that the CRA is taking to address the breaches, to notify, and to mitigate risks to Canadians.

[*Translation*]

There have been ongoing discussions related to the breach report but also pertaining to the February 2024 investigation report, given the linkages between both. Indeed, the CRA confirmed that, of the 31,393 incidents, approximately 15,000 related to the CERB fraud incidents that were mentioned in our Special Report to Parliament.

In the context of our ongoing engagement with them, on October 25, 2024, the CRA notified my office of approximately 3,200 additional material breaches that occurred in 2023 and 2024 and were assessed retroactively.

[*English*]

This fall, the CRA sought and ultimately obtained an exception from the Treasury Board, so that it could report individual cases of unauthorized use of taxpayer information by a third party to the TBS and to my office on a quarterly basis, instead of within a seven-day period, for operational reasons.

I indicated to the TBS that while I would support this exception, I recommended that it be for a limited time period of 12 months; that the CRA be required to promptly notify and provide information, support and advice to affected individuals; and that the breach reports include additional details including how and when affected individuals were notified and what additional actions were taken by the CRA to improve personal information safeguards.

On October 29, 2024, following the receipt of a complaint, I launched a formal investigation. This investigation will determine whether the CRA met its obligations under the Privacy Act and whether it employed adequate safeguards and breach response processes.

The privacy breaches at the CRA, both in the earlier credential stuffing investigation and in the one more recently reported, underscore the risk to personal information and the importance that must be placed on addressing and mitigating all breaches, including cyber-incidents.

My office regularly engages with federal institutions by providing advice and helping to assess the privacy impacts of new programs and technologies, following up on the response to breach incidents, resolving situations that were raised through privacy complaints, and conducting investigations. Each engagement and compliance activity plays an important role in supporting and advancing privacy protection across the Government of Canada, which is increasingly complex and significant in this digital era.

[*Translation*]

This includes advice and guidance to support organizations in addressing and mitigating the risks posed by breaches, including on how to prevent, contain and report breaches, as well as the importance of notifying affected individuals.

Data breaches represent one of the most significant threats to personal information globally. In the 2023-2024 fiscal year ending on March 31, 2024, my Office received over 350 reports of cyber incidents, the vast majority, or over 90%, from private-sector organizations.

[*English*]

This year, I launched investigations into other major privacy breaches. These included the Ticketmaster breach that impacted over half a million Canadians, as well as a joint international investigation with my counterpart, the United Kingdom Information Commissioner, into the 23andMe data breach, which involved sensitive DNA data.

We know that breaches can occur even when organizations have put safeguards in place. This is why an effective response to a breach is also critical to mitigating the impact on Canadians and preserving trust in their institutions.

Given the significance of these risks and the potential impacts they can have on individuals, timely breach reporting requirements need to be made a legal obligation under the Privacy Act rather than a Treasury Board Secretariat policy requirement, as they currently are.

In 2023, the OPC requested and obtained additional temporary funding as part of budget 2023 to deal with breaches. While this request was for temporary funding for a two-year period, I believe that permanent funding is required, as breaches are a permanent and growing concern that pose a significant threat to individuals and organizations.

In a digital world where the risks are higher than ever, investing in privacy is crucial. Privacy protection must be embedded throughout government programs and services.

● (1605)

[*Translation*]

We must also continue to progress on efforts to modernize Canada's privacy laws, both the private-sector law and the Privacy Act, which predates the Internet.

I also commend the committee's continuing valuable work in this area, including its report on the federal government's use of technology that can extract data from mobile devices and computers. Another example is the report released just today on regulating social media platforms to ensure online privacy and security.

We also need to ensure that my office is adequately resourced, given the increasingly complex data landscape.

This will continue to be a priority for us, and I will look forward to your committee's report on this important issue and many others.

Thank you, and I would be pleased to answer your questions.

The Chair: Thank you, Mr. Dufresne.

[*English*]

We're going to start with Mr. Chambers.

Before we do, we got off to a half-hour start. If there is no objection from the committee, I am going to reset the clock, as we normally do, at the top of the hour to give Mr. Villemure and Mr. Green six minutes each. That should take us to about 5:30. I expect we're going to get through the first round. The committee will determine where we want to go from there.

Mr. Chambers, you're up for six minutes.

Mr. Adam Chambers (Simcoe North, CPC): Thank you, Mr. Chair.

Commissioner, deputy commissioner, thank you for appearing at committee. Thank you for your responsiveness on a couple of issues that I personally reached out to your office on, including this one.

We had a bit of confusion around the timeline when we had CRA officials here. If I understand you correctly, can you confirm when you were made aware of the number of breaches dating back to 2020? Was that May 9? Is that correct?

Mr. Philippe Dufresne: That's when we received the formal notification of those breaches. Treasury Board policy requires that a formal notification be given to my office within seven days of the organization being made aware of it. In this case, clearly, this didn't happen, because some of those incidents date back to 2020.

Mr. Adam Chambers: There was obviously a large time delay. CRA officials acknowledged that they were aware of these breaches. In fact, testimony suggests that for many of these breaches, the minister was made aware, and that they were not reported in a timely fashion. After that, did I hear you right? In October, CRA officials petitioned Treasury Board to actually not report breaches on the basis of a seven-day period. They actually want more time and to do it on a quarterly basis, is that correct?

Mr. Philippe Dufresne: Yes, for some of them, that is correct. They identified that it was operationally challenging for them to do that. They requested this exception. As I indicated, I was prepared to support it with some conditions.

The three months and seven days may not make a big difference, but the seven days and three years that we're talking about in this instance is a major concern. Again, if it's for specific operational reasons and for a specific amount of time, that's a different question. The concern that we see, and we saw it, in fact, even in this earlier investigation of the GCKey, which we reported on in February. Even then we had some concerns about being notified and getting responses in time.

It's a concern, not just for CRA. That's why it should be a legal obligation.

Mr. Adam Chambers: That's very good advice.

Do you think there's an accountability issue within the department about who maybe owns the reporting and accountability requirements within CRA? I'm just trying to understand how, on one hand, a department would acknowledge that it knew these things were happening in real time but, on the other hand, would fail to properly notify or follow the rules that had been set out.

Mr. Philippe Dufresne: What we hear is that there's a focus from the departments on notifying the individuals, and that's a good thing. That's important, and you need to contain the breach. I don't know the reasons we were not notified formally by the deadline, but what I do know is that it's a concern. If we're not notified in time, we can't provide advice and guidance in time, and that elevates the risk for Canadians.

I also know that if something is required by law, there's a greater likelihood that it's going to be complied with than if it's required merely in policy or directive.

● (1610)

Mr. Adam Chambers: As part of your investigation, will you be looking at the activities that gave rise to the breach? We've heard some conflicting reports about whether it was a third party or whether it may have been on the departmental side. Is that something you'll be exploring?

Mr. Philippe Dufresne: We want to understand what happened. We want to understand whether the measures were sufficient. We need to have the context. If there were some third parties who were involved in this situation, then we're going to look at that. If it raises questions under private-sector or public-sector privacy law, then we'll address that and see whether we need to amend the scope of the complaint.

Our position is that if the government is contracting with third parties from the private sector, the government has an obligation to make sure its third party partners are providing adequate protection.

Mr. Adam Chambers: What obligation would, say, the department have to notify the public generally about potential breaches or risks to their own...if it's from one particular third party or some kind of similar instance? In this case, the public was not notified at all. I acknowledge that the individuals, some individuals, were contacted, but the general public was not made aware either.

Mr. Philippe Dufresne: There are really three categories.

You notify the individuals because you need to protect them, and you need to make sure they can protect themselves. You need to notify the regulator, which is my office. Finally, you need to notify Treasury Board and others.

However, the question of notifying the public then becomes a question of trust. How do you make sure the public isn't learning of this from the media while considering that the individuals may also be learning of this from the media? In fact, I think this was discussed in earlier testimony.

There's also a taxpayers' ombudsperson, and there's a taxpayers' charter, and one of the principles in it is also that taxpayers be notified promptly if there are fraud schemes and so on, again, for the reasons that this is important for trust and it's important to manage the stress level of individuals.

Mr. Adam Chambers: Do you feel empowered? Does your office have the right authorities to make recommendations on internal processes and accountabilities?

Also, I recognize this Treasury Board exemption, and I'll call it an exemption, but if you've just gone through a very difficult period where you've not reported, I find it a bit hard to imagine that the answer to that is giving the entity more time to report. You'd think it'd actually be the other way around: “No, you're on remedial actions, and you need to report more frequently.” I think that would make a bit of sense.

Mr. Philippe Dufresne: That's right, although I think there's something to be said about acknowledging a challenge in meeting a requirement, explaining why and seeking an exception. I think it's better than breaching it and not doing anything and not saying anything about it. I think that's an important element.

To your question, yes, our investigation will look at that. We'll make some recommendations, as we did in the earlier investigation. Our earlier recommendations included improvements in communication and accountability. We found in that earlier case that there were departments pointing fingers at each other and saying, "It's not us; it's this department or that department." We found that was an issue and had to be corrected.

Mr. Adam Chambers: Thank you very much.

The Chair: Thank you, Mr. Chambers and Mr. Dufresne.

I'm going to go to Ms. Shanahan now for six minutes.

Go ahead.

Mrs. Brenda Shanahan (Châteauguay—Lacolle, Lib.): Thank you very much, Chair.

I want to thank you, Privacy Commissioner, for being here, and I want to tell you how much we appreciate your work and how important your work is becoming.

I think it's something that I can remember when I first met with the commissioner occupying your role seven or eight years ago in the context of a committee and this vague idea of privacy, but now we understand very much what that means. It means an individual's personal information that can be used by others, bad actors, to defraud either the persons themselves or other entities.

This is where we're beginning to understand there's not just one type of breach of privacy, so correct me: What are the different types of breach-of-privacy data breaches that we can see? What do they look like? Please refer to the one at CRA.

Mr. Philippe Dufresne: We can see different situations. One could be an employee snooping. Someone is looking at information that isn't theirs. They're not entitled to it. There's not enough security around that. We also saw, in the investigation, credential stuffing. Someone finds out your password, and you're using that same password with many accounts and devices.

● (1615)

Mrs. Brenda Shanahan: Would they have found it out from the CRA, or would they have found it out from innocent citizens, somehow?

Mr. Philippe Dufresne: There could be a number of factors. You could have a situation where they find it out from individuals, third party vendors or other sources. Then it's reused.

Mrs. Brenda Shanahan: It's not from the CRA.

We're looking at what this incident is right now. Was it the CRA that somehow divulged people's passwords to bad actors? Is that what we're looking at?

Mr. Philippe Dufresne: That's not what it seems to be, at this stage.

We're going to be investigating and reaching our conclusions. It's a situation where it appears passwords were obtained elsewhere, then used to gain access to some of the devices.

Mrs. Brenda Shanahan: I have concerns about the My Account system. I rely on it. Many family members do. Many of my constituents do.

Do you have any reason to be concerned about the CRA My Account system, where people can go online and see their income tax information?

Mr. Philippe Dufresne: In our subsequent investigation, we'll look at all of the circumstances and make a recommendation.

One of the big issues we had in our previous investigation was the authentication of users and the fact that there is a lack of multifactor authentication. That was because the sensitivity and risk were assessed to be too low. That is one of the trends we see. It's not just in this instance but also in other instances. There's a sense that harm to individuals is not being treated at the level it should be. They said, "Well, you're just losing some money. It's not your health."

That was an instance when we disagreed. We said, "Well, this is being assessed at a level 2 risk. We're assessing it at a level 3 risk." In fact, if a fraudster takes $1,000 from you, you can get sick from that. You can get stressed about that. You can end up in major situations—owing money, going to court and all of those things. We found this is a level 3 risk. If you treat it as a level 3 risk, you're going to put in place level 3 protections, with multifactor authentication.

Mrs. Brenda Shanahan: It's interesting to see that it's gotten to that level of complexity.

I've certainly seen multifactor authentication. You go and put your password in. It says it's sending you a code. You have to run and get your phone. You get the code and all of that sort of thing. That is a step in the right direction. It's very good.

Someone could somehow get a hold of a taxpayer's information or password, and set up a bogus tax return. Isn't that what we're talking about? It takes time for the CRA to determine whether it is indeed a bogus tax return. You file the tax return. There's a deadline going up to April 30. There is the time for processing. Then there is the time—I think this is what you're referring to—for the CRA to contact the taxpayer.

Are these the cases you have seen?

Mr. Philippe Dufresne: The CRA is in contact with the taxpayer. They inform them and provide them with that information. At that time, there's advice about what to do.

Mrs. Brenda Shanahan: Okay.

However, there's still a question for the CRA about whether or not it was indeed the taxpayer who filed that tax return. They're taking a measure on their side. I think anyone who has dealt with the CRA knows they're very thorough in how they do this.

Would that not explain the delay in reporting the number to your office, and why they need to have the additional time?

Mr. Philippe Dufresne: I think the time starts to run once you figure out there's been a privacy breach and a real risk of significant harm.

Mrs. Brenda Shanahan: They talked to the taxpayer. The taxpayer is aware, as the person most involved. The taxpayer is providing proof, saying, “No, that was not me,” or, “What is this?”

It's true that, in secondary and other steps, maybe they talk to the public at large about some sort of scheme going on. Very often, that's the case. The same modus operandi is repeated.

Would you say that your office was in touch with officials at the CRA during this time? Were they trying to determine if this was a one-off, or whether it was indeed the tens of thousands it turned out to be?

The Chair: It's over the time, but I will let you respond quickly, Mr. Dufresne.

Mr. Philippe Dufresne: We've been in touch with the CRA in the context of this investigation and since, but we received the formal breach notification only in May. Our exchanges have been good and collaborative, but the concern is the delay in providing that formal response and those details to us as per the policy.

● (1620)

The Chair: Thank you, Mr. Dufresne and Ms. Shanahan.

[*Translation*]

Mr. Villemure, over to you for six minutes.

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

I would also like to thank Mr. Dufresne and Ms. Gervais for being with us.

My colleagues have asked a lot of questions about how this works. They looked at the “how”. I would like to talk about the “why”.

At the outset, you mentioned that it was a matter of trust.

Philosophically speaking, trust means you don't need to prove something. However, in cases of invasion of privacy, you have to prove it every time. The obvious conclusion is that there is a lack of trust.

Is this the first incident at the CRA that you're aware of?

Mr. Philippe Dufresne: No. As I said, the results of an investigation into privacy breaches of 34,000 people through the GCKey system were released in February 2024.

At the time, we made a number of recommendations and found a number of issues, including that the CRA and government organizations had not sufficiently assessed the risk level.

A big issue is understanding how serious this is and the impact it has on people. It's not a conceptual thing. Fraud in the thousands of dollars causes stress and can have an impact on health. It also has an impact on people's time, because the money needs to be recovered and so on.

We found that security had been lacking, so we recommended that it be increased through multifactor verification.

We also found communication problems between decision-makers and departments. We then made several recommendations, all of which were accepted. I have to say that there was excellent co-operation with the agency during that time, and there still is.

Nevertheless, a breach occurred, and the necessary corrective measures must be taken.

Mr. René Villemure: In your opinion, are problems related to personal information on the rise among government entities?

Mr. Philippe Dufresne: We're seeing a general increase. We see that the number of attempts is increasing and that the repercussions are more serious. According to last year's statistics, even though the number of incidents was about the same, twice as many Canadians were affected. Last year it was 12 million. This year it was 25 million.

We see that governments and departments are prime targets. At my office, a number of investigations are under way, one of which concerns privacy breaches at the Department of Foreign Affairs. Another one is about public servants who suffered a significant breach related to relocation support.

That is a trend seen all over the world.

Mr. René Villemure: You said you made recommendations that were all accepted, which is good news.

Is there good co-operation with government entities in general?

Mr. Philippe Dufresne: The entities co-operate well with us. We have regular meetings with the CRA on privacy breaches and privacy issues.

Our overall investigation of the incidents from 2020 to 2023 found that there was sometimes a lack of co-operation among the departments themselves. Representatives of a department could say that the responsibility didn't lie with them, that Shared Services, for example, was responsible, or the Treasury Board or the Revenue Agency. We stated in our report that working in silos was a problem.

It doesn't matter to Canadians which department is responsible for the problem. They deal with the government and need solutions. One of our recommendations dealt with that very subject.

However, we are still seeing, as I said, that the official notifications of breaches are unfortunately still coming to us too late and that the seven-day deadline set out in the Treasury Board policy is not being followed.

Mr. René Villemure: I'm glad to hear that there is co-operation, but it's unfortunate that they work in silos. We've talked about that a lot. People do, in fact, deal with the government.

Professor André Lareau, who appeared before the committee, talked about the ombudsman and the Taxpayer Bill of Rights. He said that, unfortunately, the burden of proof usually lies with taxpayers. Also, there is no point having the right to contact the ombudsman when it's meaningless. These are good tools, but they don't seem to be working.

Do you have a comment that would expand on that idea?

Mr. Philippe Dufresne: As you say, people can turn to the taxpayers' ombudsman, François Boileau, who is an excellent colleague. However, he does not have the power to issue orders. I agree that the ombudsman should have only the power to make recommendations, but that power is not as effective as the power to issue formal orders. The power to make recommendations is persuasive and important. The recommendation is often followed, but not always. If it isn't, the redress process becomes more complicated, when there is one.

However, the ombudsman produced a report on the Taxpayer Bill of Rights and on communication with taxpayers, as well as a very significant report on the importance of communications.

● (1625)

Mr. René Villemure: I saw a parallel when you said that a reprimand could be given through a regulation. It is not legally enforced. It's just a directive. The logic is the same, in that there is regulatory power, but no power to impose penalties.

Earlier, you talked about risk levels. We often read about a "serious breach", for example. Could you explain to us what the various levels involve?

Mr. Philippe Dufresne: Are you talking about the various breach levels, for example when I was talking about levels 2 and 3?

Mr. René Villemure: Yes, that's correct.

Mr. Philippe Dufresne: In our report, we laid out the methodology used by the government to determine the risk level and the verification level required.

In this specific case, the departments considered it to be a level 2, which required verification, but not multifactor verification. That is what allowed the breach to occur. We said in our report that level 3 is related to situations that cause moderate harm, both financially and health-wise. We indicated that, in our opinion, the potential loss of thousands of dollars could certainly have a considerable impact on people, including on their health. They get stressed and they struggle. Financially, people could have their wages garnished and then have to go through a process.

Mr. René Villemure: Would you be able to provide us with the breakdown?

The Chair: Mr. Villemure, your time is up.

[*English*]

Mr. Green, go ahead for six minutes, please.

Thanks.

Mr. Matthew Green (Hamilton Centre, NDP): Mr. Chair, I just want to note that I'm on a parliamentary server, and it's saying that my Internet is slow, so if I glitch, it's certainly not because I'm not using the appropriate technology.

The Chair: You're cutting in and out. I can hear your voice, but the video is awkward.

Mr. Matthew Green: Okay. Does it still seem to be cutting in and out?

The Chair: The voice is working, but the video is freezing a bit.

Let's see where it takes us, Mr. Green, and we'll go from there. Okay?

Mr. Matthew Green: I'll do the best I can. If the voice is fine, I'm just going to roll with it.

The Chair: Yes. Go with it.

Mr. Matthew Green: Mr. Dufresne, I'm going to ask some fairly direct questions.

There have been lots of questions about the consumer impacts. The concerns I have are actually about your delay in adequately informing Parliament.

What rationale do you have for deferring the inclusion of the 31,468 material privacy breaches until the next reporting period?

Mr. Philippe Dufresne: We were informed of half of those 30,000, so we were informed of 15,000 of them at the end of our investigation into the GCKey matter, and we presented a special report to Parliament on this matter in February 2024. Those 15,000 were made public and were included in that report, and that report was included in our annual report to Parliament.

What we did not include was the fact that we received a formal notification of this from the department, and that was because we did not receive the formal notification of this in the fiscal year. That formal notification year happened after the period we're reporting on in our annual report, so that's why that number was not in those statistics.

Mr. Matthew Green: Given the scale of these breaches, why was there no effort made to provide an interim or supplementary report to Parliament?

Mr. Philippe Dufresne: We included our special report to Parliament in our annual report. The information on this major investigation into the CRA, including the fact that there were these 15,000 additional breaches of which we received late notification, was part of our annual report. However, the updated information that we then received after the end of that period was not included because it was not in that fiscal year.

● (1630)

Mr. Matthew Green: Why not then provide an additional adequate report? Would you not agree that 15,000 material privacy breaches are, in fact, material to the accountability of Parliament?

Mr. Philippe Dufresne: The annual report was filed in Parliament in June. Parliament rose, and then we were into September and we were finding out more about the situation. Of course, we received the complaint in October, and we announced that complaint immediately.

Mr. Matthew Green: From my perspective on this committee, I've worked with you, alongside you, for many years now. I am concerned that we don't, as opposition members at least, have timely information.

You referenced, I believe, in your opening statements that, given the significance of these risks and the potential impacts they can have on individuals, timely breach reporting requirements need to be made a legal obligation under the Privacy Act, rather than a Treasury Board Secretariat policy requirement.

Would you not agree that the same duty of candour and legal requirement as a reporting mechanism to this particular committee would help to make sure that these significant issues are communicated properly?

Mr. Philippe Dufresne: Certainly I agree, and we're going to be looking at how we can improve on this. This was reported to Parliament in June. We were finding out more about the situation subsequently, and a month or so after the House returned, we announced the launch of our investigation on this, but we'll certainly be reflecting on that in the future.

Mr. Matthew Green: Yes, I would put to you that we can deal only with the information we have. The governing side has the information; opposition does not. We look to you as an arm's-length arbitrator of this type of oversight, working in partnership with this committee to help provide oversight.

When can we expect, moving forward, that you will be able to provide recommendations or some kind of reflection or learning from that gap in reporting that occurred between the knowledge of the breaches, what you called the fiscal cycle, the lack of an interim report, and then, of course, your annual reporting?

Mr. Philippe Dufresne: Certainly I think that this will be part of the report that we issue in our investigation into this matter, because we do, as we did in the previous GCKey report, talk about when we were notified, the circumstances, when the complaint was launched—

Mr. Matthew Green: Let me ask you a more direct question just for the benefit of this, because we might be ahead of you on this, given that we're doing this study right now.

What three reflections can you offer this committee to ensure to us, as recommendations for the study that we're doing right now, that timely reporting will come to this committee that will give us full information on these types of material privacy breaches?

Mr. Philippe Dufresne: I think the early reflections are, looking back at the GCKey investigation in 2020, that it was made public by the Treasury Board. The government department made it public, and then we launched an investigation after that. I think that's probably the preferred solution at this stage, but certainly we'll be reflecting on how this can be done in the optimal way with government departments, my office and this committee.

As I say, we issue annual reports. We issue special reports to Parliament from time to time. We'll look at all of those tools and mechanisms, but I think early thoughts would be that this should be something that the affected department makes public to Canadians.

Mr. Matthew Green: Would you agree that the delays affect our ability to provide timely parliamentary oversight?

Mr. Philippe Dufresne: I think that any delay has an impact on any oversight, so certainly, the earlier the information is made available, the better.

Mr. Matthew Green: Thank you so much.

Thank you, Mr. Chair.

The Chair: Thanks, Mr. Green.

That concludes our first round. We're going to go to our second round of five minutes, and I'm going to go to Mr. Caputo.

Go ahead, Mr. Caputo, for five minutes.

Mr. Frank Caputo (Kamloops—Thompson—Cariboo, CPC): Thank you very much, Chair.

I appreciate the two of you being here today for a couple of hours to answer the questions.

I'm relatively new to the committee, so I don't have the knowledge that some of my colleagues do. I'll launch into a few questions, but forgive me if I'm asking some background questions to acquaint myself.

The minister appeared here November 21. You saw the minister's testimony. Is that correct?

● (1635)

Mr. Philippe Dufresne: Yes.

Mr. Frank Caputo: Was there anything you disagreed with when you saw the minister's testimony?

Mr. Philippe Dufresne: As I say, my position is that my office should be notified within seven days of those events unless there's an exception that's granted. That's a key point that I would say. I haven't heard that. I don't know if that's a disagreement, but this is something that I would want to see as a legal obligation.

Mr. Frank Caputo: The minister should be taking action to do her job and notify you when there are these pretty significant breaches.

Mr. Philippe Dufresne: Well, I think it's all departments. It's certainly my position that this should be done. It should be a legal obligation. That will allow us to provide input earlier and better.

Mr. Frank Caputo: The reality is that when there's a privacy breach, it shouldn't take a law to require a minister to tell the Privacy Commissioner that something bad happened. We can agree on that, certainly.

Mr. Philippe Dufresne: Well, I would hope. I would hope, but experience shows otherwise. Experience shows that we are not given these formal notifications within the seven-day time.

Mr. Frank Caputo: What I find disappointing, Commissioner, is the impression that I got from the minister's testimony: We did everything we could. There's nothing to see here. This is on someone else or on something else.

Would you agree with that assessment? Would you agree that this was how the minister was portraying things?

Mr. Philippe Dufresne: I think the testimony will stand for itself. What I am saying is that I understand that departments have lots of pressure, but these notifications are important. If it were a legal obligation in the Privacy Act, with a timeline, I think we would see greater compliance in those notifications.

Mr. Frank Caputo: As I understand it, in your report of findings you made several recommendations that CRA has agreed to implement. Was CRA using best practices at the time to prevent these sorts of privacy breaches?

Mr. Philippe Dufresne: That was one of the substantive issues in the investigation. They took the position that they were. Ultimately, we found that the practices were not sufficient. We discussed this in our special report, talking about some of the advice that had started to be made and some of the concerns that were raised.

Certainly, we didn't see situations of bad faith or anything like that, but there is disagreement about the level of risk, the importance and the measures that need to be put in place here. In our report we made recommendations to elevate those security processes.

Mr. Frank Caputo: Unfortunately, incompetence doesn't require bad faith. You don't have to deliberately try to be incompetent, but there could still be incompetence there.

I'm really interested in what you just said, that CRA believed they were doing a good enough job. Am I correct in saying—I'm paraphrasing here—that they weren't doing a good enough job, and that the upshot or the corollary of the fact that they weren't doing a good enough job is that now we have 31,000 breaches? Is that fair to say?

Mr. Philippe Dufresne: Well, there will be a second report on this other situation, but we found in this first report that there was an underevaluation of the significance of those breaches for individuals, which resulted in an underprotection. We made comments and recommendations on that. We also found that there were information-sharing gaps and accountability gaps. We made a number of recommendations to improve the processes.

Mr. Frank Caputo: Again, from what I'm deducing here, and this is just my summary, CRA and the minister thought they were doing a good job. They weren't. At the end of the day, privacy breaches occurred. Now you have told them what they need to do to fix this in order to prevent this in the future.

Thank you, Chair.

The Chair: Thank you, Mr. Caputo.

Mr. Housefather, you have five minutes. Go ahead.

Mr. Anthony Housefather (Mount Royal, Lib.): Thank you, Mr. Chair.

I imagine, Mr. Dufresne, it's your job to tell agencies of the government all the time what it is they're doing not well enough and to give them corrective actions to take. Is that correct?

Mr. Philippe Dufresne: Yes.

Mr. Anthony Housefather: Each time you're doing that, you're not necessarily insulting them and telling them they're doing a horrible job and it's the minister's fault, right?

Mr. Philippe Dufresne: That's right.

Mr. Anthony Housefather: Thank you. I just wanted to correct what Mr. Caputo had said.

Let me come back to multifactor authentication, which I think is a very important question. I read your February analysis. Obviously, multifactor authentication should be almost the most self-evident thing the CRA should do. Has CRA now properly included—as it seems to me from your report that it has—multifactor authentication in all the places it should?

● (1640)

Mr. Philippe Dufresne: It has. I think there's still some time for them to finalize some of the recommendations we put in place. Ms. Gervais can correct me, but the multifactor authentication has been put in place. That issue is now resolved.

Mr. Anthony Housefather: That's good.

Are you aware of other government departments right now, based on the assessment you made using a three versus a two, that are also underassessing the problems for Canadians if privacy information gets misplaced?

Have you sent a letter to everyone to say they should be using multifactor authentication, based on a revised assessment?

Mr. Philippe Dufresne: When we tabled our special report on the GCKey matter in February 2024, we were talking about CRA, ESDC and others. Part of that special report is to be a message to all departments and all of government to say that these are the lessons they should all take.

Any department that is applying this framework should look at this in coordination with Treasury Board and adjust that calibration. My expectation would be that all departments took notice of that decision and would be implementing it.

Mr. Anthony Housefather: Are you aware of any other department that has proactively communicated with you about this report and has said that it will now do multifactor authentication?

Mr. Philippe Dufresne: We've been in touch with ESDC and the CRA. I don't know if we've been notified by other departments that they are doing this. Again, my expectation is that they are, because we've made this finding public, stating that these are our expectations for the government.

Mrs. Gervais, do you want to add anything?

Ms. Isabelle Gervais (Deputy Commissioner, Compliance, Office of the Privacy Commissioner of Canada): I was going to very quickly add that as part of the GCKey investigation, 23 other organizations that were using GCKey were also interviewed. They would have been made very well aware. The 23 organizations that we also met are listed in our report.

Mr. Anthony Housefather: Thank you.

[*Translation*]

Have you considered sending a letter to the departments to ask them the question, follow up, talk about the February report and ask them if they realize how serious the situation is and have started the process of ensuring that information is protected?

Mr. Philippe Dufresne: Yes, we could certainly consider that. In our discussions with them, process improvements and process communications were mentioned.

We are going to follow up to make sure that it is, in fact, done and that people are notified in compliance with procedure.

[*English*]

Mr. Anthony Housefather: Excellent.

On the other point that I wanted to raise.... In reading the report, it sounds very much to me like the issue is not necessarily the computer systems themselves, although the computer systems themselves can be compromised by not having things like multifactor authentication. It's more about people who are stealing private information about people on the dark web and creating new accounts for them. It's about getting access to their existing accounts using information that they've circulated, which is different from, for example, the other problems that might exist with Trojan horses and other defects in the system itself.

I have read that in the United States, about nine years ago, such an issue existed. What has happened since then is that private companies that are working with CRA would share information with CRA to work together to safeguard everybody's information. It doesn't seem like that process has started in Canada at all.

Is that something that you have recommended to CRA, and would we need to made changes to our laws to allow those companies and CRA to share information to better create a more secure overall system?

The Chair: I do need a fairly quick response, if you don't mind, Mr. Dufresne.

Mr. Philippe Dufresne: I think we made our recommendations for the situation we investigated in this one, and we'll be making more recommendations, as the case may be, in this next investigation.

The Chair: Thank you both.

Mr. Villemure, you have two minutes and 30 seconds.

[*Translation*]

Mr. René Villemure: In your opinion, has telework contributed to the situation at the CRA and could a lack of direct supervision be at fault?

● (1645)

Mr. Philippe Dufresne: We have not found that so far in our investigation. In the upcoming investigation, we'll see if that comes out. Our findings focused on the risk assessment and the time it took to detect the problem or contain the breach. We found information and communications, and we saw that the approach was possibly siloed.

We didn't approach the situation from the perspective of whether telework played a role. That said, if telework contributes to creating silos, that is a concern for us. We heard about the importance of communication among stakeholders, accountability and a team approach. Determining which departments are at fault is less important than getting good results for Canadians.

Mr. René Villemure: It may be the consequence of telework, but telework itself is not the problem.

The CRA believes that its systems were not compromised and that scammers got their hands on information from the dark web. That's what it claimed.

How credible is that?

Mr. Philippe Dufresne: I won't comment on that.

Our ongoing investigation will verify all that, and then we'll write a report.

Mr. René Villemure: The CRA said they should have had a reporting process in place.

Isn't it a little late to make that kind of observation?

In today's world, personal information gets compromised. Obviously, privacy is a fundamental right. When I hear that from the CRA, I think it should have been done beforehand.

Mr. Philippe Dufresne: As in our previous report, when we investigate a situation, we check what happened and make recommendations.

In our February report, we acted decisively to make a series of recommendations on what we saw as shortcomings. We'll do the same thing in this case, if necessary.

Mr. René Villemure: Okay.

In your opening remarks, you mentioned the use of Telegram and social media.

I don't know that side of it, so can you explain to me what role Telegram plays?

Mr. Philippe Dufresne: I don't think I mentioned the word “telegram”.

Mr. René Villemure: Okay, I must have read it somewhere else.

That said, does social media play a role in this type of situation? Does it have repercussions or consequences?

Mr. Philippe Dufresne: What we focus on is when departments use social media and providers, and information is published on social media.

This kind of situation has been investigated before. It was not related to the CRA, but to Home Depot. The information would be shared on Facebook, and people would get an electronic receipt instead of a printed one. Social media played a role in that case.

Mr. René Villemure: I realize I made a mistake when I mentioned telegram.

Thank you, Mr. Dufresne.

The Chair: Thank you, Mr. Villemure.

[*English*]

Mr. Green, you have two and a half minutes, please.

Mr. Matthew Green: Thank you very much.

Mr. Dufresne, you mentioned that it is the responsibility of the Treasury Board Secretariat to provide notice of material breaches. I'm on the secretariat's website. I don't see any major announcements of the CRA breach. Can you refer to where they would have made this public?

Mr. Philippe Dufresne: I was having difficulty hearing you, Mr. Green, but I think, if I heard you correctly, that you're asking about the announcement made by Treasury Board of the breach situation. This was made in 2020 vis-à-vis the GCKey breach. It was a statement from the—

Mr. Matthew Green: I'm sorry. I believe you mentioned that in your reporting you would have reported the additional 15,000 material breaches. That would have gone to the Treasury Board. Presumably, the Treasury Board would have notified the public. Is that correct?

Mr. Philippe Dufresne: In our "Special report to Parliament", we mentioned the 15,000 cases that we had been informed of at the end of this investigation. This special report was tabled to Parliament, so this special report is public.

Mr. Matthew Green: Do you ever take it upon yourself to do press conferences? How do you communicate to the public when big events like this happen? Is it just that you table a report and then it's our responsibility to make it public? What is your mandate to inform the public?

Mr. Philippe Dufresne: Well, from time to time, we do press conferences. In this instance, we did not. There's no set practice as to—

Mr. Matthew Green: What might be an example of a previous press conference that you would have done regarding privacy breaches?

Mr. Philippe Dufresne: We've done press conferences reporting on our investigation into Home Depot with respect to the sharing of email receipts. We did a press conference on our special report on our investigation into Aylo, the owner of the MindGeek pornographic website.

● (1650)

Mr. Matthew Green: Why those and not the CRA?

Mr. Philippe Dufresne: We made these two special reports in February 2024. We reported this alongside another of our investigations, which normally we would have reported in an annual report. This was a new practice under the Privacy Act—

Mr. Matthew Green: How did you report it?

Mr. Philippe Dufresne: There's more of a practice under the private sector legislation to make press conferences.

Mr. Matthew Green: How did you report it?

Mr. Philippe Dufresne: I'm sorry?

Mr. Matthew Green: How did you report it in February with a press conference?

Mr. Philippe Dufresne: We reported the private sector cases with press conferences because the private sector legislation gives me the authority to make matters public if I determine that there is a public interest in doing so. In the private sector—

Mr. Matthew Green: Do you have that with the public sector?

Mr. Philippe Dufresne: Excuse me, sir?

The Chair: We're having a tough time hearing you, Mr. Green. Just speak up a bit if you can, please, just quickly.

We're over time, but I'm giving you a chance here.

Mr. Matthew Green: I'm curious to know if he has the same mandate for public sector Crown agencies or departments.

Mr. Philippe Dufresne: For the public sector, it's more restricted. The public sector legislation says that I have to keep things confidential, unless I'm presenting a special report to Parliament or an annual report to Parliament. Private sector legislation gives me more leeway, which is why we've been doing press conferences with the private sector legislation. For the public sector, we've been reporting to Parliament.

The Chair: Okay.

Thank you, Mr. Green. I allowed a lot more time on that one, because I thought it was an important response from Mr. Dufresne.

Mr. Chambers, I'm going to go to you for five minutes.

Mr. Adam Chambers: Thank you, Chair.

Commissioner, I just wanted to follow up on what I thought was a reasonable recommendation by my colleague Mr. Housefather with respect to comparing what happens in the United States, in particular with its tax service, the IRS, and the close coordination it has with industry in identifying, communicating and trying to plug the holes in the dike, if you will, and in shutting down some of what I'll call these "account takeovers" or whatever...privacy breaches in general. That same kind of coordination doesn't seem to exist here.

Do you think that it would be in your remit to make some recommendations to government to explore the opportunities it has to work with third parties to address these issues?

Mr. Philippe Dufresne: I think so, and we've made recommendations in the past in terms of the public sector use of private sector service providers and what some of the parameters are. What you're referring to is coordination, participation and partnership with those and perhaps with other organizations. I think it's absolutely within my remit to make recommendations to say that these are some of the best practices we want to see.

Mr. Adam Chambers: Just to help me understand, if the privacy breach that occurred with respect to these 31,000 cases was a result of an individual company's policies, and if it was aware of that, then that company would have an obligation to report that breach to you. Is that correct?

Mr. Philippe Dufresne: Private sector organizations do have an obligation to report breaches to us.

Mr. Adam Chambers: Right. Just on that point, has any private sector organization made a report to you about this particular breach?

Mr. Philippe Dufresne: I'll look to.... About this private sector—

Mr. Adam Chambers: About the breach at CRA....

Mrs. Isabelle Gervais: No.

Mr. Adam Chambers: Okay.

When the CRA says that it's a third party and when the company in question says that it's not aware of it, but if the company in question has an obligation to report these privacy breaches, then it would make sense to believe that it could be some other nefarious third party that had access to this information. Is that correct?

Mr. Philippe Dufresne: I don't want to speculate, because we're going to be investigating all of those things. This will be our opportunity to get to the bottom of it.

Mr. Adam Chambers: That's fair enough. We look forward to your recommendations.

Do you think that maybe this committee should make recommendations or that the CRA should consider changes to its performance pay and compensation structure with respect to privacy, given how great of a concern or how important it is for Canadians?

Mr. Philippe Dufresne: I think that every tool that can improve privacy compliance is a good one. Performance management tools are good tools, because they focus the minds of executives, so I would be supportive of that.

Mr. Adam Chambers: Okay, thank you.

In this general scope of privacy, which I've written to your office about before, this is perhaps a slightly different question, but I feel it's on topic, and I haven't had a chance to speak with you about it. Do you think it's in the public interest for members of Parliament as legislators and for the public to have a full understanding of how many individuals received the private, personal, confidential details of individuals who had their bank accounts frozen as part of the Emergencies Act invocation?

● (1655)

Mr. Philippe Dufresne: Are you asking if it's in the public interest to...?

Mr. Adam Chambers: To find out how far and wide that information went....

Mr. Philippe Dufresne: I think there are situations perhaps where timing would preclude that, because you want the organization to safeguard the information, so there are situations in which you're going to wait a little before making something public.

Ultimately, as a lesson learned, I think it's something that—

Mr. Adam Chambers: That's good. I'm getting at this because the government claims that it sent these very private details, including previous convictions and licence plate numbers, to 50 organizations. A couple of those organizations, in particular the Ontario Securities Commission and the Mutual Fund Dealers Association of Canada, then went on to send that information to upwards of thousands of individuals, but we actually don't even know how far and wide that information went.

I'm just trying to understand. For me, it would make sense that we know the processes that led to it, and how far and wide.... I just wanted your opinion on whether you think the public has a right to know and whether Parliament has a right to know.

Mr. Philippe Dufresne: It's important to know how far the breach went and how widely the information was shared. Was it appropriately done? Were there some valid reasons, and were there some valid contractual or other protections? Those are the things we're going to be looking at in our investigation.

Mr. Adam Chambers: Thank you very much for your testimony.

The Chair: Thank you, Mr. Chambers and Mr. Dufresne.

I'm going to go to Ms. Khalid now, for five minutes.

Ms. Iqra Khalid (Mississauga—Erin Mills, Lib.): Thank you very much, Chair, and thank you, Commissioner and deputy commissioner for being here today. We really appreciate it.

I just want to clarify. H&R Block previously said in a statement that there was no evidence that the breach came from its firm. The tax firm said that a comprehensive internal investigation had concluded that none of its data systems, software or security had been compromised. H&R Block said it was not aware that any of its own clients were impacted by the breach.

Do you have any information that would confirm that?

Mr. Philippe Dufresne: I can't speak to that, because we have launched an investigation. That's what we're going to be looking into.

Ms. Iqra Khalid: You will be getting to the bottom of where exactly the breach occurred. Is that right?

Mr. Philippe Dufresne: Yes.

Ms. Iqra Khalid: As we go through this digital age, the nature of nefarious actions is different. In so many ways, the more we are public, the more we try to find that balance between raising public awareness and battling the crimes as they're occurring. The changes are so fast as technology changes.

Where do you think that balance is in terms of public protection and public awareness?

Mr. Philippe Dufresne: I think it is a balance. Organizations need to work together. This is the importance of early notification, bringing all of the key players around the table, including my office and the Canadian Centre for Cyber Security. Dealing with all of those different perspectives is important in order to bring lessons learned to parliamentarians and Canadians.

There are many tips in terms of changing your passwords and being aware of those things. Ultimately, we want organizations to have very strong privacy protection mechanisms to diminish the load on individuals.

Ms. Iqra Khalid: What do you think the nature of that relationship should be? Who is ultimately accountable here?

Mr. Philippe Dufresne: Ultimately, departments, governments and private sector organisms that control the information are accountable for it. They have legal obligations under the Privacy Act. They have legal obligations under the private sector privacy legislation. In the private sector, those obligations include notifying regulators, getting input, getting advice and getting best practices.

We're seeing that the public and private sector are aware of this. People are seeing the cost and the harm. We need to do more to be more successful.

Ms. Iqra Khalid: I appreciate that.

Recently, the government hosted an auto theft summit, which dealt with many of these similar issues. As digital technologies are used more and more in vehicles, it makes it easier for them to be stolen, for example. Bringing all of industry, different levels of government and police together led to some really significant steps forward.

Who do you think should be at the table if we were going to have a conversation like this with respect to privacy, especially regarding the breach we're talking about today?

● (1700)

Mr. Philippe Dufresne: Make sure you have the experts, like the Canadian Centre on Cyber Security. Make sure you have the regulator—in my case, my office. Make sure we are consulted. Make sure we're involved early on. This is why I recommended that privacy impact assessments be done and made a legal requirement. This should be done publicly, because it will raise confidence.

There's a role in working even beyond our sectors. I'm working very closely with the Competition Bureau, the CRTC and the Copyright Board. Wherever there are these commonalities, partnership collaboration is always going to be beneficial.

Ms. Iqra Khalid: Lastly, can you help us understand the differences between the roles of ministries, departments and agencies as they engage with you?

Mr. Philippe Dufresne: Their obligations are similar in the sense that they all have the obligation to protect personal information they have and that Canadians entrust them with. They need to ensure they have adequate safeguards. They need to ensure they work with my office and Treasury Board to report in a timely way and be responsive to the recommendations.

It's an important obligation, because it goes to the trust of Canadians. Those breaches have significant impacts on Canadians.

Ms. Iqra Khalid: Thank you very much, Commissioner.

Those are all the questions I have.

The Chair: Thank you, Ms. Khalid and Mr. Dufresne.

We're going to reset the clock here.

I am glad you brought up the issue of H&R Block, though, because that had not been brought up to this point. I'm equally glad to hear, Mr. Dufresne, that they are part of the investigation, because they were implicated in this. In fact, the motion that was passed by this committee was to have H&R Block come here to answer questions. We received correspondence from them, as committee members know, to say they have done their own internal investigation and found that it wasn't their issue. I look forward to your report on this to see if they were involved at all and if the information of Canadians was not breached as a result of their mechanisms as well.

This is a six-minute round. This will take us to about 5:30. I'm going to leave it up to the committee to decide whether they want to go past this point.

Mr. Barrett, you have six minutes. Go ahead.

Mr. Michael Barrett (Leeds—Grenville—Thousand Islands and Rideau Lakes, CPC): In 2020 you made several recommendations to the government. Do you believe the recommendations you made are being followed by the government?

Mr. Philippe Dufresne: I do. Some of them have a 12-month implementation period. My sense is that they are on track to meet them.

Mr. Michael Barrett: Would the implementation of any of those recommendations prior to this point have prevented the breach that occurred?

Mr. Philippe Dufresne: We're going to be looking into that in our current investigation, so I can't speak to that.

Mr. Michael Barrett: Is it your view that privacy breaches should be immediately brought to the attention of Canadians?

Mr. Philippe Dufresne: There are situations when you might need to keep something confidential because you want to address it, you want to contain it and you don't want the threat actors to have the information. There is a balance there.

Certainly, it's important that my office be made aware in a timely manner and that the discussion about public communication to do that take place as soon as possible.

Mr. Michael Barrett: A news report on this matter says:

> According to sources, the crisis prompted the CRA to contact the office of Revenue Minister Marie-Claude Bibeau.

> The agency prepared media lines to respond to inquiries should there be questions about the breach of H&R Block data and why the agency paid out millions to scammers.
>
> In the end, the public was never alerted to the scheme.

The scenario that you described, sir, was to help contain the threat, perhaps, take action and inform your office immediately, before then informing Canadians. This looks like a government not protecting Canadians but protecting itself from the criticism of Canadians who were the victims of, potentially, the government's negligence—likely the government's negligence, in fact.

Do you believe it's acceptable for the minister to have withheld this information from Canadians?

Mr. Philippe Dufresne: I think my office should have been notified earlier than it was. I think it's beneficial for Canadians to have information as soon as possible. There may be circumstances in which it needs to be kept confidential longer. I point to the 2020 situation, when the Treasury Board made a public announcement on this, so Canadians were aware of the earlier situation.

● (1705)

Mr. Michael Barrett: Right.

In this case, they didn't. They literally just prepared a damage control plan and didn't inform Canadians, whose personal information was being used for the ill-gotten financial gains of fraudsters and criminals.

Isn't there an ethical and a moral obligation for a minister, acting on behalf of the Crown, to inform Canadians?

Mr. Philippe Dufresne: In terms of best practices, I would want to see notifications to my office, and I would want to see notifications—

Mr. Michael Barrett: That didn't happen. Your office was not notified.

Mr. Philippe Dufresne: We were notified, but late. We were notified—

Mr. Michael Barrett: Quantify that.

Mr. Philippe Dufresne: We were supposed to be notified seven days after the department became aware. We were notified in May 2024.

Mr. Michael Barrett: How many days later was that?

Mr. Philippe Dufresne: Some of those breaches dated back to 2020. We're talking many, many days.

Mr. Michael Barrett: Continue with your answer.

Mr. Philippe Dufresne: I think public information is important so that lessons can be learned. There was a public announcement by the Treasury Board in 2020 on the GCKey matter. We investigated it. We issued our recommendations. These are publicly available statements and conclusions that helped the public debate and draw conclusions.

Again, subject to some confidentiality provisions, which may be legitimate for a certain time, these matters should be made public.

Mr. Michael Barrett: The Canadians who have been defrauded would rightly lose confidence in the institution of government generally.

Also, in this case, the Canada Revenue Agency has extraordinary powers and extraordinary access, and can be the vector by which individuals end up jailed or fined, have their wages garnished and assess massive penalties. This organization—this minister—opted instead to lie by omission to Canadians. Canadians were expected to believe that everything was okay, because they weren't told any different.

Does it cause irreparable harm to the institution of government when this information is concealed from Canadians?

Mr. Philippe Dufresne: What we highlighted in our earlier report is that these breaches have impacts on Canadians. They can cause stress. You highlighted garnishing. There can be situations in which people have to take very distressing steps.

As much as possible has to be done for Canadians in these circumstances, in terms of informing them, notifying them and protecting them—and in terms of drawing lessons from that.

Mr. Michael Barrett: In my remaining time, Chair, I want to give notice of a motion:

> Given that, at a time when Canadians are lining up at food banks in record numbers and facing the worst cost of living crisis in a generation, Justin Trudeau's Minister of Emergency Preparedness accepted two taxpayer-funded VIP suite tickets to attend a Taylor Swift concert in Vancouver, the committee:
>
> 1. call on the Minister of Emergency Preparedness and PavCo Chair Gwendolyn Point to testify before this committee for no less than two hours, separately; and
>
> 2. order PavCo to provide the names of all federal ministers, officials or staff provided with tickets to any of the Taylor Swift concerts at BC Place, and any related communications.

The Chair: Thank you for that, Mr. Barrett. The motion is on notice. That concludes your time.

Mr. Fisher, you have six minutes. Go ahead, sir.

Mr. Darren Fisher (Dartmouth—Cole Harbour, Lib.): Thank you, Chair.

Thanks to the witnesses for being here. I really appreciate their very focused answers. It has really helped in a situation in which not everybody has a depth of understanding.

Some of the things I've scribbled down here may seem like they're not in any specific order. They're things that were said during your discussion today.

What is “credential stuffing”?

Mr. Philippe Dufresne: Credential stuffing is when you reuse passwords you obtained from other sources. You're using these, as a bad actor, to gain access to websites and portals. It's essentially to gain access to information.

Mr. Darren Fisher: Obviously, we know data breaches are on the rise. I think you were speaking about your office having to continuously adapt. You talked about some one-time funding and a need for that to be more permanent.

Can you tell me a bit about how you are, as an office, continually adapting to this increase in data breaches?

● (1710)

Mr. Philippe Dufresne: We have made these funding requests to Parliament. We obtained temporary funding. We will be continuing to push for this to be permanent, because those breaches are not diminishing. We're looking at processes, right now, within the OPC. One of my three strategic priorities is to protect and promote privacy with maximum impact. We're looking at our structures. We're looking at whether we are putting enough resourcing in the compliance side of the office, including breach protection. We're asking for more permanent resources.

We're also looking internally to see how we are structured and operating. We're looking into our technological knowledge. We have a technology lab, and we're continually developing our expertise there. We're working with international partners and partners in Canada—the privacy commissioners in the provinces and territories, and international partners. I indicated that I launched an investigation, along with my colleague, the UK commissioner, into 23andMe. That's an investigation into another major breach.

We're leveraging each other's expertise. We're learning from each other. Breaches and cybersecurity are themes we're discussing more and more in the privacy community here in Canada and around the world.

Mr. Darren Fisher: Thank you for that.

You talked about some of your recommendations—improving communications, incident response plans and accountability.

How have reporting procedures and methods changed because of these events—or have they?

Mr. Philippe Dufresne: The measures have changed because of the recommendations we made in that investigation.

CRA and ESDC have taken steps. They've put multifactor authentication in place. They have worked on their processes, assessments and communication frameworks. Some of those recommendation elements had a six-month timeline. Some of them have a 12-month timeline, so they're not all completed. However, they're on track to being completed. That's what we want to see when we make recommendations. In this case, the departments agreed with our recommendations and accepted they had to implement them. We want to see that.

We'll see what this next investigation results in. If there have been some shortcomings, there will be more recommendations, and we would expect the same collaboration and compliance.

Mr. Darren Fisher: MFA, or multifactor authentication, was brought up by Mr. Housefather, and I think a few other people mentioned it as well. If MFA had been present, would that have prevented this particular breach or this set of breaches?

Mr. Philippe Dufresne: We found that in the investigation we did on the GCKey in 2020, in many cases it would have provided additional protection, which would have prevented the breach. Without it, it's all too easy to gain access.

Mr. Darren Fisher: It's funny: Whenever I have to enter a site that has MFA, I always groan and lament the extra process I have to do, but after this conversation and after this ethics meeting today, I'll be much more willing to entertain that extra step of using MFA, based on some of the things you've said.

Mr. Darren Fisher: What improvements, additionally, that have not been talked about today would you like to see made to better coordinate different government agencies in protecting the confidential information of Canadians?

Mr. Philippe Dufresne: There are a number of things that we'd want to see.

I talked about breach reporting. We need to see this as a legal obligation in the Privacy Act.

We need to see order-making powers for my office. This is something I don't have at the moment, and that adds potential delays. If you have a department that agrees with the recommendations, that works, but if it doesn't, then we need to go to court, and that adds delays and costs.

I want to see privacy impact assessments made mandatory and not just Treasury Board policy, because privacy impact assessments are also part of the solution to this. It's early risk assessment of new programs and new tools, so this is important.

We want to see necessity and proportionality as requirements under the Privacy Act. They're not currently, but they're requirements for the private sector. There should be similar standards of protection for the public sector and private sector.

As well, there should be collaboration between different offices. One of the challenges currently in Canadian privacy law is that I cannot do a joint investigation with my colleague, the competition commissioner of Canada, but I can do that with the U.S. FTC. That's a gap. We need more of that collaboration, including to deal with breaches.

● (1715)

The Chair: Okay, that's time.

Thank you, Mr. Dufresne.

[*Translation*]

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

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

A lot has been said, and I won't make you repeat what you've said so far. However, I'll come back to my first point.

What intrigues me enormously, in situations like this, is the reasons why this has happened and continues to happen. I understand that there are more users, more apps, more platforms, etc., but I don't know why. When it comes to ethics, it's often said that a change made to the structure without addressing the culture is doomed to failure. Why do these things keep happening?

They're going to keep happening. What could be done to improve the situation?

Mr. Philippe Dufresne: I believe that the contribution of your committee, through its reports and recommendations, as well as the contribution of my office, through its investigations and recommendations, are important. In fact, on our side too, we're taking a close look at public communications and user-friendly tools.

We need to reinforce the importance of privacy not only in general, but also in the more specific context of breaches. We sometimes tend to see this as a very technical issue. Yes, we don't like complicated passwords or multi-factor authentication. However, it's important to understand why this is important. In the world we live in, a lot of information is transmitted over multiple platforms, so we need to develop the reflex to realize that when information is compromised, it has a major impact on people.

These are lessons we can already draw from our first report. We told the people in charge that they were underestimating the impact it has on people. We also told them that, when the problem arises, you can't point the finger at one department or another. We're a team and we need to find solutions.

Mr. René Villemure: I often come back to privacy education. I'd even go so far as to say that the public isn't necessarily very literate when it comes to privacy, and that there's still an educational mission to be fulfilled here.

It seems to me that we might prefer to have a law rather than a directive, but the fact remains that it would be a measure used to right wrongs rather than to prevent breaches in terms of culture. I often put the same question to the Information Commissioner: does the government have a culture of opacity or transparency? She answers that it has a culture of opacity.

In this case, transparency wasn't there either, and I find that worrying, because it prevents us from having a culture of accountability.

Mr. Philippe Dufresne: I think one of your recommendations, in the report you just tabled today, concerns privacy literacy, and I support it. Equipping people is very important. With my provincial and territorial colleagues, I'm discussing the idea that there should be mandatory privacy courses in schools. It should be part of the learning process. The more tools we can give people, the better.

However, I also think that we shouldn't relieve organizations of their responsibilities. So it's not just a question of equipping people. It's also about organizations making privacy as easy as possible for people.

Mr. René Villemure: This last point really resonates with me. I understood from the minister's testimony, when she came here, that the burden of proving anything was on the user. So, in the name of accountability, the organization is disengaging, which I find unacceptable. Literacy is certainly necessary, but it doesn't take responsibility away from the other party.

What you say about compulsory courses at school reminds me of the days when there were home economics courses. We laugh about it today, but it was important at the time. It seems to me that courses on the importance of privacy as a fundamental right should be compulsory.

Mr. Philippe Dufresne: I agree with you. We and our international partners reported this summer on deceptive cookie and consent form practices. We found that these practices were widespread. Complex language and psychological tools are being used to push people into making choices that are not good for them and that will make them reveal too much information.

So we need to better equip people to recognize such practices and challenge them. Organizations must also continue to do their part to make it easy for individuals to protect their privacy. It may never be easy, but it has to be easier than it is right now.

● (1720)

Mr. René Villemure: I seem to spend a lot of my evenings managing parameters and unchecking boxes. If there are too many, the average citizen gets annoyed. If they don't understand what they're doing, they get annoyed too. I think you first have to understand what you're trying to protect. The means may not be the right one, but the fact remains that there are many deceptive practices. I still think that, after a while, people get tired of ticking boxes.

Mr. Philippe Dufresne: Absolutely. In fact, in our Home Depot survey, we found that when people asked for an e-mail receipt instead of a printed one, the information was communicated to Meta. However, this was not indicated at all to customers at the checkout. One of the company's responses was that it was in their policies on their website and that customers could find this information there. We told them it wasn't acceptable to put such a burden on people, and that it wasn't part of people's reasonable expectations to have to research this extensively before giving consent. This kind of practice leads to consent fatigue.

Recently, we won our case against Facebook over its consent practices. The Federal Court of Appeal pointed out that the texts on which Facebook's consent practices were based were often longer than an Alice Munro short story. It's complex and doesn't help users understand what they're consenting to.

Mr. René Villemure: Plus, it's often written in legal language.

Mr. Philippe Dufresne: Yes, that's right.

Mr. René Villemure: Thank you very much.

The Chair: Thank you, Mr. Villemure and Mr. Dufresne.

I was told there would be no further questions from the Conservative and Liberal parties. Mr. Green's intervention will therefore be the last one of this meeting.

[*English*]

Mr. Green, you have six minutes. Bring it home.

Mr. Matthew Green: Wow. I'll take it somewhere. I don't know if it will be a Conservative slogan, but—

Voices: Oh, oh!

The Chair: That's okay. Please conclude.

Mr. Matthew Green: Thank you.

Mr. Dufresne, you mentioned that there's a different mandate for public disclosure for private companies versus public agencies or departments. Why is that the case?

Mr. Philippe Dufresne: For the public sector, under the Privacy Act, I'm mandated to keep confidential the information that I received in my mandate, unless I'm making it public in an annual or a special report to Parliament, so there's a limit. In the private sector legislation, I also have to keep it confidential, but the act gives me the authority to make it public if I determine that making it public is in the public interest. That is the authority we regularly use to make private sector matters public, including with press conferences, so that's the practice.

In fact, the practice of the OPC used to be that, once a year, all of the public sector complaints were made public through the annual report. I decided to change that this year, because I felt it was too long to wait an entire year before making these things public. That's why we started doing special reports, including in this matter—to make it public to Parliament. I take the point, perhaps, of having more press conferences, and these should be done as well.

Mr. Matthew Green: I appreciate that. I'm going to reclaim my time. It's scarce.

What you described was the mandate, so, within your mandate, you are following the rules of the mandate. I would ask you this, given that this is a government that claims it wants to have a culture of transparency: Would it not be helpful to have equal consideration for disclosure of privacy breaches, regardless of whether they are private sector or public sector? In your opinion, what's the benefit of not having that in a mandate for both sides, public and private?

Mr. Philippe Dufresne: There's no benefit. I agree with you absolutely, Mr. Green. This is something that should be amended in the Privacy Act. We've been calling for legislative amendments to the Privacy Act for some time. It's a 40-year-old piece of legislation. This should absolutely be one of the changes.

In the meantime, I've started to use this special tool of doing a special report to Parliament, and we're going to reflect as to whether we can do more, including press conferences.

● (1725)

Mr. Matthew Green: I would put to you, in quasi-legal terms—my friend called it lying "by omission"—that it's a material non-disclosure. The public has a right to know when there are breaches, whether they're caused by private third parties like H&R Block or through an agency like the CRA. As we've heard, they have profound impacts on Canadians, people who were embroiled in potential fraud allegations and people who would no longer get access to their GIS or their OAS. It's a significant thing. I'm happy to hear you before committee, recommending that we provide that within your mandate.

You also mentioned your ordering powers. Can you expand on that a bit and on why it would be important to demand full disclosure and not have obstruction from, I would call them, belligerent departments?

Mr. Philippe Dufresne: I'm sorry; I didn't hear the last part of your question.

The Chair: I'm sorry, Mr. Green. I've stopped your time.

There is a little bit of chatter on all sides here. I want Mr. Dufresne to hear Mr. Green clearly.

Mr. Green....

Something's going on with his microphone; it's kind of muted. I've mentioned it to the clerk before.

Mr. Green, please restate your question for Mr. Dufresne, and then I'll start your clock after that. Go ahead, sir.

Mr. Matthew Green: I appreciate that, Mr. Chair. I'll speak a little bit louder. Maybe that'll help.

I'm happy to hear that you're calling for this recommendation. You also mentioned the importance of having greater powers, order-making powers, so that if there's administrative sabotage or departmental belligerence in not wanting to co-operate with your investigations, having greater powers within your commission would allow more timely reporting. Can you expand on why that's so important?

Mr. Philippe Dufresne: It's important, because we have seen many situations where we receive these reports late, as we did in this instance. That creates the types of situations that we've seen here. It prevents us from giving advice early on and from working with the organizations early on. If this is a legal obligation, I am convinced that there will be greater compliance with this with public sector institutions. It's a legal obligation for private sector organizations. It should be a legal obligation for public sector organizations.

Mr. Matthew Green: In keeping with that spirit, do you feel that you have adequate penalties or deterrents, administrative deterrents, for people who fail to comply or are repeat habitual offenders in breaches? Do you have enough power within your commission to hold real accountability?

Mr. Philippe Dufresne: I do not, because, for both the private sector and the public sector, I do not have order-making powers, and I do not have the ability to issue fines. Those are recommendations that we've made to Parliament for both the public sector and the private sector. It's being proposed in Bill C-27 for the private sector. I would want to see this, certainly, in an upcoming bill dealing with public sector privacy law.

Mr. Matthew Green: You mentioned recommendations from the 2020 GCKey debacle, from your study on that. You mentioned that some of them had made some progress. In your opinion, were there any recommendations that weren't followed that may have led to the continued gaps in the administration of privacy on this most recent breach by the CRA?

Mr. Philippe Dufresne: That will be part of what we assess in the investigation in terms of seeing what happened when, and whether the recommendations that we made in our GCKey report mattered. When were they implemented, and did these things occur before or after, for instance, the multifactor authentication and the improvements in terms of the process and verification? That will certainly be part of our conclusions in this upcoming investigation.

Mr. Matthew Green: That concludes my questions.

Thank you very much, Mr. Dufresne, for being here.

Thank you to the committee for struggling through my IT issues. I hope to have those resolved for the next meeting.

Thank you.

The Chair: Thank you, Mr. Green.

That concludes our round of questioning.

Mr. Dufresne and Ms. Gervais, on behalf of the committee, I'd like to thank you for being here today and for accommodating us. I know we had a bit of difficulty last time, but we made it through this time.

You might as well settle in, Mr. Dufresne, as you're coming back Tuesday on the TikTok issue. I appreciate your making yourself available to this committee for back-to-back meetings.

That concludes the meeting for today. I want to thank everyone, including the clerk and the analysts.

I will advise the committee that you did receive an email from the clerk with respect to questions that have been asked of Twitter, or X. That should be in your email right now. Keep an eye out for it.

Thank you, everyone. Have a great weekend.

The meeting is adjourned.

Published under the authority of the Speaker of the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the Copyright Act. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the Copyright Act.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website at the following address: https://www.ourcommons.ca

Publié en conformité de l'autorité du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la Loi sur le droit d'auteur. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre des communes.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la Loi sur le droit d'auteur.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes à l'adresse suivante : https://www.noscommunes.ca