HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 032 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, November 1, 2016

Vice-Chair

Mr. Joël Lightbound

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, November 1, 2016

● (1100)

[*Translation*]

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

Welcome to the 32nd meeting of the Standing Committee on Access to Information, Privacy and Ethics.

We are fortunate to have with us today the Privacy Commissioner of Canada, Mr. Daniel Therrien, who is accompanied by Ms. Sue Lajoie, director general, Privacy Act investigations, and Ms. Patricia Kosseim, senior general counsel and director general, legal services, policy, research, and technology analysis branch.

Welcome and thank you for being here.

We have an hour and a half. We will begin with a presentation by Mr. Therrien, for 10 minutes, followed by questions from MPs.

You have the floor, Mr. Therrien.

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

Thank you once again for your invitation and your decision to conduct this important review of the Privacy Act.

I would also like to thank all those experts who have testified before you thus far.

As you have heard from many expert witnesses, the 33-year old Privacy Act is woefully out of date.

Over the past few years in particular, technological developments have been revolutionary, making the collection, use and sharing of personal information by governments much easier.

Last spring, I had recommended amendments to the Privacy Act under three main themes: legal modernization, technological innovation, and the need for transparency.

I stand by these recommendations, but would like to make certain clarifications today.

Many witnesses have asserted, particularly from the provinces, that there is much to be said for a regime of privacy protection that includes binding orders issued at the conclusion of certain investigations.

In my appearance last March, I indicated that the current ombudsman model needs to be changed as it often leads to delays. Furthermore, under the current regime, departments do not have a strong incentive to make complete and detailed representations at the outset, and the current model does not therefore result in a timely, final remedy.

The ombudsman model has been in place since the OPC's inception in 1983. This means in part that I can be both a privacy champion, as well as investigating complaints. These are both vital roles in the protection of privacy and I was concerned that legal reasons would force me to choose one over the other. Specifically, the concern was that the courts would deem that I would not be able to adjudicate complaints impartially if I am also a privacy advocate.

After careful review, last summer in particular, we have concluded that there are indeed legal risks with one body having both adjudicative and promotion functions. Based on our review, however, these risks are likely the same under the hybrid model in Newfoundland and Labrador.

Importantly, crucially in fact, our review also led us to conclude that these risks can be largely mitigated through a clearer separation of adjudicative and promotion functions within the OPC.

This kind of structure, as you know, exists in many provinces. It is important to understand that such a separation would entail certain costs, but we have not yet quantified these.

Since the legal risks and mitigation measures are the same under the hybrid model in Newfoundland and Labrador, the order-making model is in my opinion preferable as it provides a more direct route to timely, final decisions for complainants.

Therefore, as I wrote to the committee in September, I now recommend that the act be amended by replacing the ombudsman model with one where the Privacy Commissioner would be granted order-making powers.

[*English*]

In your committee's report on Access to Information Act reform, several recommendations appeared that were consistent with the policy to promote open and transparent government.

I agree completely with this policy as a cornerstone for public trust and accountability, but I suggest that it should be pursued in a way that protects privacy. As I mentioned several times, the Access to Information Act and the Privacy Act are to be seen as seamless codes, and changes to one act must consider the impact on the other. Changes to the way in which access and privacy rights are balanced under the current legislation should be carefully thought through, including any changes to the definition of personal information, and changes to the Access to Information Act's public interest override.

In my view, these changes should be considered in the second phase of Access to Information Act reform. I was therefore happy to see that your report in June on access, if I read it correctly, did not recommend changes that would affect that balance.

Now here's a word about risks if reform is not pursued. There will be, in my view, real consequences if Canada does not modernize its privacy legislation.

● (1105)

In the public sector, these consequences include, first, risks of data breaches that are not properly mitigated; second, excessive collection and sharing of personal information, which may affect trust in government; and more specifically, third, a reduced trust in online systems that may undermine the government's efforts to modernize its services and coordinate its digital communications with Canadians.

Some governments have already moved forward to strengthen their privacy protection frameworks, most notably the European Union. There is a risk, in my view, that if European authorities no longer find Canada's privacy laws essentially equivalent to those protecting EU nationals, commerce between Canada and Europe may become more difficult. This is not theoretical. This is what happened to the United States when the safe harbour agreement was found invalid by EU courts a few months ago.

Since I last appeared before this committee in March, the Federal Court recently considered the Privacy Commissioner ad hoc mechanism that my office created to provide for an independent review of complaints against my own office. This mechanism was needed when the OPC itself became subject to the Privacy Act with the adoption of the Federal Accountability Act in 2007. In assessing the independence of this mechanism, the court noted this was a question more appropriately addressed by Parliament. I would therefore invite the committee to consider this issue at this point, and we've added this to our revised list of recommendations.

In conclusion, I wish to thank and congratulate the committee for undertaking this critical work, which I hope will lead to a modernized law that protects the privacy rights of all Canadians. We hope that the government will see fit to take action on all of our recommendations.

Since the government has confirmed its intention to amend the Access to Information Act in two stages, we would ask that the following recommendations to the Privacy Act, at a minimum, be part of phase one.

First, an explicit necessity threshold for the collection of personal information should be adopted, so that the easier collection made possible by new technologies is properly regulated in a way that protects privacy. Second, an obligation to safeguard personal information and a breach notification provision should be made explicit in the act, to ensure the risk of data breaches is properly mitigated. Third, a requirement for written information-sharing agreements, with prescribed minimal content, should be adopted to improve transparency.

Finally, amendments consequential to phase one amendments to the Access to Information Act should be made, including replacing the ombudsman model with one where commissioners are given order-making powers to ensure that individuals receive timely, final decisions to their complaints.

Thank you for your attention. I welcome your questions.

[*Translation*]

The Vice-Chair (Mr. Joël Lightbound): Thank you very much for being with us again this morning, Mr. Therrien. Thank you for your presentation.

I think the MPs have a number of questions for you. We will begin with Mr. Raj Saini, for seven minutes.

[*English*]

Mr. Raj Saini (Kitchener Centre, Lib.): Thank you, Mr. Therrien, for your opening remarks.

Last week, we heard from several departments. I want to ask you this question specifically because I want to make sure that we understand where the Privacy Act or where the impact should begin. There's one specific case where you helped the RCMP with their drone surveillance program, where you were involved at the outset of that program.

We got some differing answers, but when departments are going to have a rule, regulation, law, or whatever, where do you think your department could be best implicated in making sure that the act or that rule...? Do you believe it should be from the beginning, and do you think that should be a necessary requirement?

● (1110)

Mr. Daniel Therrien: Yes, it should be at the beginning, and many privacy laws around the world agree with that premise.

My premise is that it is preferable to identify, reduce, and mitigate privacy risks before they occur, as opposed to finding remedies after the risk has materialized. It is important to have remedial powers, but it is just as important, and probably more important, to identify risks as programs are developed, and to mitigate these risks from the get-go.

Mr. Raj Saini: Something that I've had a particular interest in is the information-sharing agreements, not necessarily domestically but internationally. You mentioned the EU in your opening remarks. What can we do to make sure that our laws are strengthened?

Specifically, bilaterally I know that we have agreements with certain countries that have the same sort of robust regime that we do, but we may have agreements with countries whose regime is not as robust. How do we prevent any information in a secondary country from being exposed, especially for a Canadian individual?

Secondly, if we have a bilateral agreement with one country, we may not have a bilateral agreement with a third country, but the second and third country may have an agreement. How do we prevent that information from going beyond the second country?

Mr. Daniel Therrien: The question you're raising actually should make us all think about the worst-case scenario that Canada has experienced since 9/11, which was the Maher Arar case. It is important that we understand the lessons from that case and other lessons from 9/11. Here we had Canada sharing information with the United States and later on with Syria, which led, according to the commission of inquiry, to Mr. Arar being tortured by Syrian authorities. How can you mitigate that?

First of all, Canada does not have complete control of this issue. Of course that's a question of bilateral relations and bilateral agreements between countries, but Canada can certainly make its position known and prescribed in agreements by making sure that, when Canada shares information with another country, the information to be shared is identified and the purposes for which it is shared are identified, and here I do not mean on a transactional basis. It would be too cumbersome to have agreements on a transactional basis. That's not what we're recommending, but we are recommending that there be umbrella agreements that provide more specificity than the act itself on what type of information in a given context will be shared and for what purpose the information will be shared. That's one set of criteria.

As to potential sharing by the country with which we have an immediate agreement to a third country, that should also be part of the agreement with the second country. It should be provided that, in the case of Mr. Arar, an agreement between Canada and the U.S. would provide that the United States would not be able to share information with a third state unless certain conditions were met. I think that would be an important safeguard.

Will the United States or a second country always comply with this agreement? Well, that's a question of bilateral arrangements between countries. Normally, in these situations, countries try to live by their commitments. Is there an absolute guarantee that this would be so? No, but normally these commitments are agreed to, so it would be important, in an agreement like that, that the potential of sharing with a third country, particularly, as you say, one where human rights protection may not be robust, is covered in the agreement with the second country.

● (1115)

Mr. Raj Saini: How about if it comes to commercial transactions? Would you suggest something in that regard? In some cases there are Canadian companies or Canadian individuals who have interests in many countries around the world, and if certain tax information, corporate information, can be shared with another country because of a bilateral tax treaty, what would happen? How would we prevent that information, which could impact the company in Canada, from being shared with other countries or other competitors?

Mr. Daniel Therrien: I'll put it at the level of policy objective. That issue, of course, was raised in the context of FATCA, as an example. The first step, I think, is to determine whether the agreement between Canada and another state—here the United States—for tax purposes is trying to achieve a legitimate purpose. In the case of FATCA, the objective was to avoid tax evasion, which is a legitimate purpose.

In general terms, first, the purpose must be identified. Is it a legitimate purpose? Then, ensure that the information that being shared is consistent with that purpose and does not go beyond that purpose. If you follow these rules, yes, the information of certain Canadian individuals or companies may be shared, but it will be because an analysis will have been made that there is a valid policy objective to be achieved and that no more than what needs to be shared for that purpose is shared.

[*Translation*]

The Vice-Chair (Mr. Joël Lightbound): Thank you, Mr. Saini. Your speaking time is up. There will certainly be time for more questions at the end.

We will now move on to Mr. Jenereux, for seven minutes.

[*English*]

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Thank you very much for being here. I appreciate your taking the time, and I'm sure there are a lot of staff who have listened to plenty of the testimony over the months of preparing your remarks today.

You definitely hit my biggest concern on the head in your discussion on the order-making powers and your changes over the course of the year leading up to this testimony. Particularly, in March 2016, you recommended improving the ombudsman model to the investigation of complaints and wrote that the Newfoundland and Labrador hybrid model would be the best to advance the Privacy Act. Then in 2016 in a letter to our committee, you said that the adoption of the order-making powers at the federal level on balance would be preferred to the hybrid model.

You went into a bit of detail, but I want to give you the opportunity to go into a bit more on why you prefer the order-making model to the hybrid, and what led you to the decision you're at today.

Mr. Daniel Therrien: First, what is the ill to be solved? The ill to be solved is in part delay, the fact that the current model does not give sufficient incentives for government departments to provide submissions to us, and particularly well-thought-out submissions early on in the process. That leads to delays for the person who should benefit from the intervention of the Privacy Commissioner, the person who makes a complaint. The order-making recommendation is meant to give the complainant a timely response and a final response that will not drag on in the courts forever.

I've dealt with the issue of timeliness. In the current system, departments do not necessarily have to give us full submissions from the get-go. It's possible for them to make their real case before the Federal Court because we can only make recommendations but it is the Federal Court that can actually order a federal institution to do something consistent with the Privacy Act. We have seen cases where departments gave us a set of submissions in our investigation and have then augmented these submissions when they were before the Federal Court. I think that's also inconsistent with the desire to have timely final decisions for the complainant as soon as possible.

These are two issues that order making would try to address. I was originally and I am still of the view that there is a risk with order making as well as with the Newfoundland model that if the Privacy Commissioner has a promotional role, a privacy champion role, and an adjudicative role, these two roles can conflict. Our analysis over the past few months has confirmed that unless you take measures to divide certain functions internally, the courts will likely intervene and say you're not impartial when you adjudicate because you took a position as an advocate that showed how you were disposed to look at a certain issue, and you maintained that position and did not listen to the facts carefully. That's a real risk.

I was concerned with that risk from the get-go. We thought originally that the Newfoundland model could potentially offer a solution but after further review we think that actually the risk is the same whether it's order making or the Newfoundland model, so if the risk is the same, if the mitigation measures, namely division within the OPC, are the same, I'd rather have order making because between the two models it's the one that provides the most direct route, the faster route, for the person we should care about, which is the complainant.

● (1120)

Mr. Matt Jeneroux: On that note then, do you think that the commissioner's order-making powers should be defined in the act, or do you think instead that a broad discretion is more effective in exercising that power?

Mr. Daniel Therrien: It could be defined. It certainly can be defined, and it probably should be defined as meaning that the Privacy Commissioner could make orders that would direct a government institution to do what in the Privacy Commissioner's view is necessary to comply with the Privacy Act. That's ultimately what order making is all about, and of course there would be judicial review by the Federal Court after that, but in terms of administrative process that's what order making would be, so you would need to define that in the statute.

Mr. Matt Jeneroux: We had a number of the departments in front of us and they expressed a real concern about opening up requests to outside of Canada, in other jurisdictions. In particular, immigration felt they weren't meeting the particular level at this point in time. They were hitting about 60% in terms of their privacy investigations in a timely fashion, and they're worried that this would increase it more.

Have you any comments on that?

Mr. Daniel Therrien: I would start from the premise that rights under privacy should not depend on nationality; that's a policy choice. There are already mechanisms whereby even though there is no statutory right, there are mechanisms that I will ask my colleague Sue to explain that get to the same place. Essentially to give foreign nationals a right would codify and give greater stature to a set of rules, which by and large already exist. Would this create more volume and more delays? Potentially.

Sue.

Ms. Sue Lajoie (Director General, Privacy Act Investigations, Office of the Privacy Commissioner of Canada): For example, a lot of the requests Citizenship and Immigration receives for information that would traditionally be considered personal information requests are handled through the Access to Information Act. Because of some of the wording of the legislation, because the individual is located outside Canada and is not a Canadian citizen, they still have a means to obtaining the information they would need for processing their immigration file. They go through a person present in Canada to represent them and obtain that information. It's unclear how many additional requests opening the Privacy Act to a broader audience would change.

● (1125)

Mr. Daniel Therrien: In other words, to give foreign nationals a right of access under the Privacy Act wouldn't deal directly with what currently occurs indirectly when you have foreign nationals making access requests through agents under the Access to Information Act. If we're there indirectly already, let's do it directly.

The Vice-Chair (Mr. Joël Lightbound): Thank you, Mr. Jeneroux. We're well over seven minutes.

We will now move to Mr. Blaikie.

Mr. Daniel Blaikie (Elmwood—Transcona, NDP): Thanks,

At least one of our witnesses who was somewhat critical of the idea of conferring order-making power on the Privacy Commissioner said that in part it was because of the quantity of requests you get through PIPEDA. I was wondering if you think that at a certain point a difference in quantity of requests or complaints requires a qualitative difference in response. Do you think that's important, first of all, and second, do you think the office could tolerate a difference in powers with respect to the public function under the Privacy Act and the private function under PIPEDA?

Mr. Daniel Therrien: I think at the end of the day, the way in which my provincial colleagues have implemented similar schemes demonstrates that it's only the tip of the iceberg. Only the small minority of cases of complaints lean to order making. Before you get there, you try to resolve, you try to mediate, you try all kinds of things that we would try to do. I don't see why we would have a different experience from that experience in provinces where order making is a necessary tool to use in few cases. It's important to have the tool in the tool box, but in managing the volume of work and the volume of complaints, I don't think that order making would be used in very many cases.

Mr. Daniel Blaikie: In the case of having necessity tests for the collection of information, whether they're related to programs or whether it's a charter test or whatever else, how do you envision the oversight mechanism for that? Is that something your office would do? Would it largely be self-regulated by government departments, and then your office would just get involved if someone were to complain that a government department was collecting information that didn't pertain to a program? How do you see the oversight?

Mr. Daniel Therrien: First, it would start with privacy impact assessments. As government departments developed new programs that require personal information, we would engage with them at the level of privacy impact assessments, before the fact, having in mind this necessity standard to assess whether the way they propose to proceed would conform with that principle.

Once the program was in force and the information was collected, yes, we would be involved based on complaints, as is currently the case. If you agreed with our recommendations, we would be able to order departments to no longer collect or to change their practice, if we think it is not consistent with the necessity test.

Finally, the courts would be there as the ultimate arbiter. They ultimately would define the legal interpretation of the criteria that the OPC would then be bound to follow.

Mr. Daniel Blaikie: In the case of your recommendation for information sharing, that the threshold be that the sharing is necessary as opposed to reasonable, I think, is the difference. Again, I'm just curious how that would work when it comes to oversight. You mentioned a couple of cases, Maher Arar being one, where there was information sharing among governments that had negative consequences. If you were to have that necessity requirement, how do you imagine the oversight happening? Who does it and when, exactly? If the RCMP is getting ready to share information with a foreign government, for instance, do they call up your office and say this is something they're about to do? How does that oversight actually happen?

● (1130)

Mr. Daniel Therrien: First of all, necessity would apply to the collection of information. For information sharing, our recommendation is that there be agreements with certain content, which I won't go into, but necessity is not one of the conditions of our information-sharing agreements. There should still be a link between the objective of the program, the information to be collected, and so on.

Your point is how we would oversee transactions, at the transactional level, for information-sharing cases. First, we would intervene before the transaction occurs, at the policy level, at the PIA level. At the transactional level, if a department wanted to consult us and they couldn't, there's nothing in our recommendations that would require them to consult us on a case-by-case basis. It would occur before the fact, at the policy level, at the content of the agreement level. Then the department would implement the agreement. If somebody felt that this transaction did not have accordance with privacy law, he or she could make a complaint. We would intervene then.

I don't see our interacting with institutions on a case-by-case level once the rules are set.

Mr. Daniel Blaikie: Are you recommending then, in a case where, say, there is a complaint after the fact and you find that there's a breach, that there be any kind of consequence for that breach? What do you think should be the outcome of your finding in a case where it's shown that this agreement, if there is a written agreement, wasn't followed properly?

Mr. Daniel Therrien: That's a good question.

At a minimum we would find that the transaction was not in accordance with privacy law. To the extent that it's not too late to remedy the situation, one could think about how to frame the order making to provide for that situation. I don't have a precise recommendation to make, but it may be that it's too late. If it's too late, our position would govern the future. We would acknowledge, would say to the department, “This was inconsistent with privacy law; you should govern yourself accordingly.”

Theoretically, you could think in terms of damages or things like that. I'd rather try to determine whether it is too late to remedy the situation. If it's too late, I would not jump to the issue of damages. I would try to find other remedies to protect the person in the situation before the transaction, which was inconsistent with privacy law.

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

We'll now move to Mr. Erskine-Smith for seven minutes.

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

I'd like to start with your recommendation to create an explicit necessity requirement for collection. Privacy is a quasi-constitutional right. There are always two legs to a constitutional analysis. It's not just necessity; it's also proportionality. Some witnesses testified at this committee that we should impose that requirement as well, and it should be a dual requirement. I wonder if you have thoughts that we should not only make it necessary but make it proportionate.

Mr. Daniel Therrien: We say that the statutory standard should be necessity, but we also recommend that you consider defining necessity. In our recommendation we define necessity, in part, through proportionality. At the end of the day, both necessity and proportionality would be part of the standard.

Mr. Nathaniel Erskine-Smith: That requirement would be for collection. In answer to my friend's question, you had mentioned it's just for collection, but not for information sharing.

I want to talk about three different things: collection, that's pretty clear; there is also information sharing; and then there's the retention of that information and the timelines for retention. When we get to information sharing, if it's not a necessity condition or standard, we heard from some witnesses that it could be a compatible use standard, it could be a consistent use standard. What standard are we talking about? Surely there should be some condition. It shouldn't just be through ad hoc agreements.

Mr. Daniel Therrien: The current act already does have a number of standards, so consistency where it applies and then other standards in other situations. For instance, one of the provisions that authorizes information sharing is in court proceedings in order to respond to a subpoena. There's no gradation here. Either you respond to the subpoena, or you don't.

● (1135)

Mr. Nathaniel Erskine-Smith: I'm sorry to jump in, but those are specific cases and surely different standards might depart from them, so if we have a necessity requirement for collection, great. We could have another requirement generally speaking and it could be departed from in specific instances, as outlined in the act. But why would we not impose a necessity requirement for information sharing if we're imposing it for collection, at least in the first instance?

Mr. Daniel Therrien: In an information-sharing context, there are two parties. There is a sending institution and there is a recipient institution. For the recipient institution, the information-sharing transaction is actually a collection exercise, so necessity may not apply to the sending institution, but it applies to the recipient institution.

Mr. Nathaniel Erskine-Smith: In fact, necessity, then, is fundamentally for the receiving institution. The collecting institution will govern information sharing fundamentally.

Mr. Daniel Therrien: Yes.

Mr. Nathaniel Erskine-Smith: Great.

When it comes to retention of information, should we also impose a necessity requirement?

Mr. Daniel Therrien: I will say yes. Certainly, retention at the level of principles should be governed by.... Yes, the necessity to keep that information for a lawful government program, that should ultimately be the test.

Mr. Nathaniel Erskine-Smith: Perfect. Thanks very much.

Your previous recommendation had been to allow complainants to apply for review by a Federal Court, that the court be able to award remedies including damage awards. A full array of remedies, I think, was the language used.

When I look at the recommendations now, do I take it that the recommendations consider creating a statutory mechanism to independently review privacy complaints against the OPC? Is that part of it, or has that recommendation gone?

Mr. Daniel Therrien: There are two things. To deal with the easier question first on the privacy ad hoc mechanism, in 2007 the OPC became subject to the access provisions of the Privacy Act and the Access to Information Act. We had to provide information, as departments, which then led to, if according to an individual we do not act in a way consistent with this legislation, who do people complain to?

In a Privacy Act scenario, we cannot be party and tribunal at the same time, so we created this mechanism. In a case called Oleynik, which is a few weeks old, the Federal Court heard arguments as to whether there should be a statutory basis for that mechanism. They suggested this was not something the court should look at, but that Parliament should look at. That's one thing.

Mr. Nathaniel Erskine-Smith: Bracketing that and then moving to the courts as the arbiters for damage awards and a full array of remedies, has that been removed from your set of recommendations?

Mr. Daniel Therrien: Yes, essentially on the basis that here we're dealing with.... Tribunals federally are subject to judicial review, as you know. There is a special remedy in the Privacy Act, which is a *de novo* review of an access request. That's a current remedy in the act.

Why was that remedy created? We think it was created to provide a readily accessible remedy to individuals in cases where the OPC may recommend that a department disclose information but the department does not, so there needs to be an easily accessible remedy for the individual.

If the OPC has order-making powers, our position is that the need for this remedy, the Federal Court *de novo* review, may no longer be there because we would be the readily accessible remedy for individuals to have access. We're actually even more accessible, and perhaps quicker, than the Federal Court *de novo* review.

Mr. Nathaniel Erskine-Smith: Assuming the powers don't include the power to award damages, would it not still be required that an individual should seek remedies from a Federal Court?

Mr. Daniel Therrien: In our submission, then, if there were a charter violation, there would be damages according to section 24 of the charter, but otherwise not.

Mr. Nathaniel Erskine-Smith: My last question is on order-making powers. You had originally asked for a hybrid, and you've been clear that you're now asking for order-making powers. Without having tested systems at the federal level with the Information Commissioner and the Privacy Commissioner, do you think there is any merit in giving the Privacy Commissioner hybrid powers, or in seeing how a hybrid system plays out, so that we could learn from both systems in our five-year review?

● (1140)

Mr. Daniel Therrien: The short answer is no. What I think we should all try to achieve is a mechanism that provides a quick, final decision to individuals who seek access or privacy rights, together with a system that is sustainable. As to arguments around whether the hybrid model creates risks of conflicts of interest and so on, I think such arguments would simply delay things, creating judicial debates that are not necessary. I would rather deal with the issue head-on and have order-making powers.

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

We'll now move to Mr. Kelly.

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

Your recommendation number 13 asked for discretion to discontinue or decline complaints in specified circumstances. The recommendation mentions specifically frivolous, vexatious, or complaints made in bad faith, but it also talks about specified grounds that include those categories. Are there are other grounds you think would be appropriate, to be able to have discretion for discontinuance?

Mr. Daniel Therrien: I'll give you a few and I'll ask my colleague Patricia Kosseim to complete the list.

We say “including” because this kind of discretion exists under PIPEDA. We can manage our work volume, essentially, by refusing to handle certain complaints on various grounds, including if a complaint is frivolous or vexatious. There are, however, other grounds in PIPEDA. For instance, is there another effective remedy available to the individual, other than to make a complaint to the Privacy Commissioner? Is the commissioner seized of another complaint that raises the same issue? In order to be efficient, you look at one complaint, not a number of complaints. These are two of the grounds in PIPEDA.

Madam Kosseim will complete the list.

Ms. Patricia Kosseim (Senior General Counsel and Director General, Legal Services, Policy, Research and Technology Analysis Branch, Office of the Privacy Commissioner of Canada): Other grounds that exist currently and with which we work in respect of the private sector include where there's insufficient evidence to pursue the investigation, perhaps due to timeliness and the disappearance of relevance; where the organization itself—in this case, a department or an institution—has already provided a fair and reasonable response to the individual; or where the matter has already been the subject of a report by the commissioner and a recurring issue has already been dealt with. Those are some of the additional examples.

Mr. Pat Kelly: You would be required, though, to state what the specified grounds are.

Mr. Daniel Therrien: Absolutely.

Mr. Pat Kelly: What would you envision, if you have this discretion, as an appeal process when a person makes a complaint and they don't agree that their complaint is vexatious or frivolous, that it has been adequately addressed through another case, or that it is connected with or raises the same issue as another pending case?

Mr. Daniel Therrien: We would say that judicial review would be an appropriate remedy. I would say that this type of discretion exists with many tribunals. It may raise issues of access to justice, or access to a response on the merits of the complaint. I recognize this. However, many tribunals, administrative or judicial, are given the authority to balance access to justice with certain limitations where giving access to one individual might actually impede access by others. That's essentially the concept. It exists elsewhere. We recognize that there's an issue in respect of access to justice. We would not use this frequently. I think our record under PIPEDA shows that we use this infrequently, and that's essentially what we're recommending.

● (1145)

Mr. Pat Kelly: I'm not sure if I'm going to have time for a full question and answer here. Maybe we'll have to come back to this later.

For budgeting purposes for individual departments, has there been much consideration given to the effect of expanding judicial recourse and remedies? If judicial remedy is expanded, will this result in a net increase in compliance costs for various departments as well as your own?

Mr. Daniel Therrien: I don't see that our recommendations would increase judicial remedies, but if your question is what is the net effect of all our recommendations on government resources, with the chair's indulgence, I could spend a minute or two on that, or we could come back.

The Vice-Chair (Mr. Joël Lightbound): You can indulge.

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

We think order making may actually lead to efficiencies because in the process that I've described currently with recommendation making, there is quite a bit of back and forth between us and departments during the investigative process and there's no real incentive for departments to respond to us quickly and completely. We think that amount of going back and forth would be reduced significantly with order making.

Concerning the requirement for privacy impact assessments, the obligation to have safeguards and breach notification, we recognize that this may increase costs for the government. Some departments actually have these practices, so for them, there would be no cost. However, for many, there would be an increase in costs. I don't think these increased costs would be large, but they would not be marginal. I would urge you to consider these costs as an investment to ensure that the public has trust in how the government deals with their personal information in a digital world.

Mr. Pat Kelly: It wouldn't be so much a concern or suggesting that the cost ought not to be borne, but just simply for planning purposes, that the crown ought to know.

Anyway, thank you.

The Vice-Chair (Mr. Joël Lightbound): We might come back later, Mr. Kelly, but we're well over the five minutes.

We'll now move to Mr. Long, for five minutes.

Mr. Wayne Long (Saint John—Rothesay, Lib.): Thank you, Chair, and thank you, Commissioner, again for coming in.

I read some articles over the last few days about you and the department. One article I read was about metadata legislation, and you certainly have stated time and time again that you're looking for enhanced legislation, improved legislation, and certainly referenced the Communications Security Establishment and their sharing with the Five Eyes, and that some of the breaches never should have happened in the first place. I just want to get your comments on what you feel about metadata legislation and what you're looking for, moving forward.

Mr. Daniel Therrien: You refer to the example of the incident involving Canada's Communications Security Establishment. I would start by saying that the government claims—and I have no reason to dispute that claim—that metadata, particularly in a foreign intelligence context, is necessary to identify threats. I don't dispute that. The issue with the incident in question was that metadata was then shared with partners, with Five Eyes, in a way that was found by the CSE commissioner, the oversight body, as being unlawful, inconsistent with the statute.

What that tells me is that we have an activity that is legitimate, that pursues a legitimate goal, but is currently regulated in an insufficient way. What I'm looking for—to answer your question—is not a very prescriptive list of conditions necessarily, but currently we have extremely broad provisions that authorize certain institutions to collect and share metadata. I'm looking for some framework, some statutory provisions that would set out certain principles, according to Parliament, according to our elected officials, as to when government institutions would be able to collect metadata, when they would be able to share metadata, under what principles or under what conditions generally speaking, and under what conditions they should retain that information. I'm not looking for something very prescriptive; I'm looking for some basic rules.

● (1150)

Mr. Wayne Long: Thank you.

The next question I had for you is this. You were also stating that you want telcos to have more detailed police requests and you don't feel that's being done enough. Also, you commented that you were disappointed in the Canadian chiefs of police who were looking for warrantless access.

Have you seen improvement in that, or what exactly do you want there?

Mr. Daniel Therrien: For companies, we have seen that a number of them do publish transparency reports when they are the subject of lawful access or warrantless access requests by the police, so there is improvement. I think all companies involved in that area should publish transparency reports.

My main point would be that it's not enough that companies do that. Government departments, which are at the receiving end of this information, should also be more transparent and issue transparency reports. After all, it is the departments that are asking for that information for law enforcement purposes. It's one thing for companies to do it, but the ones who should really be transparent are those who ask for and use the information. I'm not asking them to reveal law enforcement secrets, things that would impede lawful investigations, but there is a way for departments to be more transparent.

I'm sorry, I lost your last question.

Mr. Wayne Long: About the chiefs of police, and I think it was the commissioner—

Mr. Daniel Therrien: Yes.

The chiefs of police, including the RCMP commissioner, make the point that the Supreme Court's decision in Spencer, which reinforced the need for warrants for access to the sensitive personal information of Canadians, is essentially creating important impediments that make their lives, if not impossible, extremely difficult, and that Parliament should provide for more cases of warrantless access if the police are to do their jobs. I need to be convinced of that. I think we all need to be convinced of that.

I don't question in any way the difficulties, in the past, of the police and national security agencies, but I think it would be important that they demonstrate what conditions in Spencer make their lives impossible. One of the conditions in Spencer is that if there is an urgent need to have access to information, it can be obtained without a warrant. If that's the case, why do they need to further liberalize the conditions?

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

We will now move back to Mr. Kelly, for five minutes.

Mr. Pat Kelly: Thank you.

Since I asked a complicated question with only a minute left in the previous round, maybe we'll let you have a bit more time to elaborate.

First, I do want to make clear that the purpose of my question is certainly not to suggest that there be a price on privacy. There are legal obligations that are very clear, and it's very clear that Canadians have very high expectations around privacy. However, when there is a change in regulation and enforcement, it's important for planning purposes that both departments, not only your own but all of the government departments and agencies that are affected, be able to plan accordingly.

You said that you think in many cases the stick that would now be wielded by your office would make departments more efficient. Did I understand that correctly?

Mr. Daniel Therrien: On the order making, there are many recommendations that we make. With respect to the change to an order-making model, for that particular recommendation, I think it is quite possible that the system would become more efficient, including for departments.

There are other recommendations that would likely create costs. I recognize that.

● (1155)

Mr. Pat Kelly: With regard to these additional costs, are they, at this stage, likely to be understood by the affected departments that may be subject to additional costs?

Mr. Daniel Therrien: It's a complicated issue.

One of our recommendations is to create a legal obligation for departments to safeguard information technologically, and there would be a breach notification provision. One would think—and there are policies in the Treasury Board and other departments that suggest a similar outcome—that departments need to do what is necessary to protect information that is given to them by individuals. At the same time, we see that there are breaches reported regularly and that departments do not always take the measures necessary to improve their systems.

On that issue, a lot of work is done in government to protect information that I think is insufficient, in terms of surpassing the bar for what would be required. What would be the cost of that? It's not as if you're inventing a new activity. It exists. We just ask that it be improved. We haven't quantified that cost, but it should be, I would say, not insignificant but not extremely important either. One would hope and one thinks that certain measures have already been taken by government to protect information.

Mr. Pat Kelly: Fairly quickly, then, I'd like to get your comments on how protections are built in around mandatory breach reporting to ensure that the act of reporting a breach does not compound damages to an affected party.

Mr. Daniel Therrien: This is something that we see in the discretionary regime currently. I think I'll ask my colleague Sue to expand on this, but this is something we see both under the privacy regime and the discretionary regime that we have currently and under PIPEDA.

Sue, do you want to expand on this?

Ms. Sue Lajoie: Currently there is already a mandatory policy requirement for institutions to report privacy breaches to our office as well as to the Treasury Board Secretariat when there is a material privacy breach that is identified in an institution. Putting it into law would probably just expand a little bit on what's already in existence. Whether or not institutions are following their policy requirements fully, that's.... We don't know what we don't know.

Mr. Daniel Therrien: That being said, you're right in that creating this obligation, whether by policy or by law, may create the risk for further increases in damages. We were consulted by the innovation department on the same policy in the private sector, and we actually made certain comments there on how to mitigate that risk. I recognize there is a risk, but it's possible to mitigate that risk.

[*Translation*]

The Vice-Chair (Mr. Joël Lightbound): We will now move on to Mr. Bratina, for five minutes.

[*English*]

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

Monsieur Therrien, in recommendation 11 you recommend amending section 64 to allow the commissioner to report publicly on government privacy issues. We've discussed this in previous testimony.

Are you satisfied with the level of independence in your office with regard to making further reports and also order-making power? Could you give me a sense of how you feel about the independence of the Office of the Privacy Commissioner?

Mr. Daniel Therrien: I don't have concerns in terms of our independence. We investigate independently. We audit independently. We have strong policy and legal units that allow us to fully look at issues with which we're confronted without having to call on government. I think we have the structure to ensure that the work we do is carried out in an independent manner.

● (1200)

Mr. Bob Bratina: So the public can be reassured that the Privacy Commissioner feels the office functions at a level of highest integrity in terms of that.

Mr. Daniel Therrien: Yes.

Mr. Bob Bratina: In terms of reporting publicly on issues, would this be a report in terms of a statement issued by the office? Would you do media interviews? How do you interact with the public in those terms?

Mr. Daniel Therrien: By any and all of the above would be the answer. We have experience with this under PIPEDA, the private sector legislation, where even though our investigations under PIPEDA are confidential, as they are under the Privacy Act, I have discretion to make public findings and recommendations outside of the context of an annual report. We do that from time to time. We issue case reports, give documents to practitioners, to experts, which is helpful to them and helpful to companies in changing their behaviour or adapting to what we say. I think that if we had similar authority to do that for the public sector, outside of the context of annual reports, this would be helpful to departments as well as providing guidance during the year.

To give an example, in my last annual report I made public certain findings on national security on the incident that was brought up by Mr. Long, for instance. That finding was made several months before the annual report. We were precluded by the confidentiality provisions of the Privacy Act to make that public in a timely way, so I had to wait until the annual report. I could have made a special report. That's another possibility, but these special reports are quite formal exercises and I'd like to be able, when it makes sense, to make public in a less formal way, but a fully informative way, findings that we make during the year.

Mr. Bob Bratina: Finally, with regard to time sensitivity and so on, we have two incidents right now, one in a province, one in the United States, of information that may seem to be influencing an election. I wonder if there are restraints around your office with regard to the election period.

Mr. Daniel Therrien: That's a good question. At the end of the day, we act independently but we act responsibly. We would certainly have regard, from the timing perspective, for the impact of our release of findings so as not to advantage any one party or the other, but on the contrary, to ensure that the publication of the finding does not influence what would otherwise be the considerations, say, in an election period.

Mr. Bob Bratina: The problem right now is that whether there's an intent to influence or not obviously there will be some influence. That's a pretty profound question the Americans are facing right now. I'd like to talk to you more about that, but I'll leave it for now.

Thank you.

[*Translation*]

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

We will now move on to Mr. Blaikie, for three minutes.

[*English*]

Mr. Daniel Blaikie: Thank you.

In your presentation you mentioned that one of the risks of not updating the Privacy Act was that our European partners, for instance, might not be willing to engage in trade within certain sectors. I just wonder if you could elaborate a little bit on what sectors could possibly be affected by that.

Mr. Daniel Therrien: I think it applies to most sectors, actually.

Under European law, part of the privacy protection given to EU nationals by European law is that the substantive protection standards provided under EU law essentially are transferred when information goes outside Europe. Europe only allows the transfer of data outside of Europe if Europe is satisfied that the protections in place in the other country are adequate, or according to a recent judgment from the European court of justice, essentially equivalent to those in place in Europe.

In Europe, an important safeguard for privacy protection is the necessity and proportionality test. When I recommend to you that collection and other activities occur on a necessity test, I have in mind the protection of Canadians primarily, but it may also be useful when Europe ultimately assesses Canada's privacy laws that we have similar concepts in terms of privacy protection.

In the safe harbour case, the European court found that the U.S. privacy protection was not adequate and was not essentially equivalent to that of Europe, and therefore, put an end to what was then the agreement under which personal information was transferred from Europe to the U.S.

Canada has the benefit of having its legislation found adequate by Europe in the early 2000s, but Europe must renew this assessment from time to time. While I'm not saying that this is something we need to have in mind for tomorrow, ultimately Europe will reassess Canada's laws, and I think we would be in a better situation if some of the main concepts of privacy protection in Canada were not a carbon copy of European law but had some equivalency.

● (1205)

Mr. Daniel Blaikie: Yes, I'm just wondering about that in the context of a trade agreement with Europe, for instance. One of the principal advantages, we're told, for accepting all of the negative consequences of a trade agreement for particular sectors, but also for the government's ability to regulate within Canada is that our companies and our businesses won't be subject to significant non-tariff trade barriers. It sounds to me that unless that's addressed in CETA, and there is a provision saying that Canada's law, whatever they may be, will be recognized by Europe, there continues to be, at least in this sense, a very significant, potential non-tariff trade barrier despite all the trade-offs for Canada within CETA.

Mr. Daniel Therrien: I haven't read CETA. I understand it's somewhat of a brick, but we will certainly do that soon.

Mr. Daniel Blaikie: Thank you.

[*Translation*]

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

That concludes the question period.

Since we have about 15 minutes left, I will open the floor to those who have other questions, starting with Mr. Massé.

Mr. Rémi Massé (Avignon—La Mitis—Matane—Matapédia, Lib.): Mr. Therrien, I have two questions for you.

First, I would like to go back to what Mr. Kelly said earlier, specifically, the financial impact and the impact on your resources of moving from the ombudsman model to that of an ombudsman who has order-making powers.

I would like to know what the financial impact will be. Will you need more resources? Have you quantified the additional costs of moving from one model to another?

Mr. Daniel Therrien: We have not quantified those costs specifically. If we obtain these powers, we would have to change our structure. We cannot ask the same public servants to conduct investigations, to serve in a promotion role, and in an adjudicative role. As a result, some employees would have one role but not the other.

At present, our office is completely integrated. For example, a group of lawyers supports the activities of the investigators, the promotion staff, and those who make recommendations to departments or companies. The same lawyers can provide advice to everyone.

If we obtain these powers, we would have to separate certain functions. The integrated structure we have now would no longer be possible. That would entail costs.

That said, we would try to limit costs. In arbitration cases, for instance, the order-making powers would be used in a minority of cases. That would be one way to limit the impact on our resources.

We have not quantified the costs specifically, but we would attempt to limit them. There would be an increase, but we do not think it would be a major increase.

● (1210)

Mr. Rémi Massé: Once you have more information and have analyzed these costs, the committee would be interested in that information.

Here is my second question.

There was an article in *La Presse* yesterday that created quite a commotion. The phone line of a journalist, Mr. Patrick Lagacé, had seen tapped, and 24 warrants had been issued. Of course this caused quite a stir in the media and in the public in general.

I do not want to judge the situation. The fact remains that it was fairly easy to get these warrants to tap a journalist's phone. People are wondering whether it is really possible and that easy to get warrants to find out what is happening just on someone's phone.

This issue concerns the Montreal police service, of course, but I would like to hear your thoughts on it. Can you comment on the broader issue of protecting privacy and access to information?

Mr. Daniel Therrien: This case is indeed worrisome. I will not get into the issue of freedom of the press, but rather, as you requested, will talk about the protection of privacy, of a journalist or of any other person.

First of all, it was metadata from this journalist that was obtained under a court order. In the Spencer case, a warrant had been obtained. So one of the conditions for the protections set out in that decision appears to have been met.

The question this raises is the following, in my opinion. There was reference earlier to certain police forces that would like to be able to obtain such data without a warrant. In the present case, the metadata were obtained with a warrant and we can question the appropriateness of this.

That leads me to suggest that you reflect on the following. Even if the courts are involved, does Parliament not have a role to play in establishing the criteria that a judge must apply before giving permission for metadata to be obtained? Freedom of the the press would certainly be one of those criteria. We can consider issues relating to the balance among various interests. What is the importance of the crime under investigation? Are the metadata obtained sensitive in nature or not?

It is one thing to say that the courts are involved and that this is a good start, but this case leads me to believe that this is not sufficient. It would probably be helpful to give the courts tools so they can more effectively exercise their powers in such cases.

Mr. Rémi Massé: Thank you very much for your reply.

That's all for me.

The Vice-Chair (Mr. Joël Lightbound): Are there other questions from committee members?

If I may, I have a few questions myself.

[*English*]

Bob, you wanted to ask a few questions?

Mr. Bob Bratina: Yes, I have a question regarding recommendation 16 on limiting exemptions to personal information access requests. It says the exemption should be injury-based and discretionary. Injury-based is simple to contemplate, but how would discretionary be applied in terms of limiting exemptions?

Ms. Patricia Kosseim: One of the examples that has been the subject of much discussion here, both in the access to information context as well as in the privacy context, is around the exemption to access to information where there's personal information involved, as an example. One of the pivotal points is how to decide what the conditions are for releasing that information, despite the fact that personal information may be involved.

Currently, the Privacy Act provides under paragraph 8(2)(m) that personal information can be disclosed if, in the minister's discretion or in the delegated decision-maker's discretion, there's a public interest in disclosing that information. There is already a discretion that exists. The question is whether that starting premise of privacy as the default is the proper premise. We think it is and we think that, certainly in the interest of privacy, we should start from that premise, but that's not to say that there isn't room for discretion to disclose when there's a public interest to do so.

● (1215)

Mr. Bob Bratina: In defining the recommendation, would the discretionary exemption still be one-offs, or would you write them in a specific way?

Ms. Patricia Kosseim: Currently, the act provides for a balancing test, with oversight from our office. On a transactional basis, if personal information is disclosed in the context of an access to information request, we will be informed of that. We can't overwrite that—that is a ministerial discretion. However, we could intervene if we think the individual should be informed of that disclosure before the disclosure actually happens.

One of the basic principles of our office is that we should look at these on a transactional basis, because the weighing of the factors will be very different on a case-by-case basis. There's not a class exemption, for instance, for personal information. Those should be treated on a case-by-case basis.

Mr. Bob Bratina: In terms of the recommendation, then, is it a drastic change from what has been in place before? I'm trying to understand it. It sounds to me like the discretion and the injury-based notion of exemptions already exist. Is this something further, just to be clear on it?

Ms. Patricia Kosseim: I think the recommendation is that where there are exemptions in the act to access to personal information requests, those should be injury-based as a starting premise. With respect to the Privacy Act exemptions, for access to personal information requests, that's the general principle that we're putting forth as the default.

Mr. Bob Bratina: Thank you.

[*Translation*]

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

Mr. Therrien, if I may, a have a few brief questions for you.

I know this does not relate specifically to the Privacy Act. I did, however, like what you said earlier to Mr. Massé about metadata. We have seen in Mr. Lagacé's case, for example, that the courts were involved. A judge issued a warrant. In your opinion and based on your expertise, what would be the best legal avenue to regulate this metadata and access to it?

I have a second question as well. In your opinion, would it be helpful to include a definition of metadata in the Privacy Act to ensure that it is treated as personal information?

Mr. Daniel Therrien: I'm not sure I have a specific answer to your question as to what the criteria should be.

Let will begin with the following. Apart from the story that was reported in the media this week, another case was heard in an Ontario court a few months ago. The telecommunications companies complained that the police had access to metadata of a very large number of people who went by a specific location. There was a telecommunications tower which made it possible for data to be transmitted to the police, to which it could have access under a warrant. The telecommunications companies asked the judge to establish conditions in the warrant in order to protect privacy.

The judge ruling on the case stated—and I think this was correct—that he did not have the legal tools to do what the companies were asking, including establishing a period of time during which the police could keep the data obtained under the judge's warrant.

In my opinion, the courts recognized that, even if they wanted to impose conditions on obtaining or keeping metadata, the current legal regime is not clear enough to give them these tools or to impose such a condition. This raises the question as to whether such conditions should be added.

What should the criteria be? I do not have a specific recommendation apart from what we have discussed thus far about criteria such as necessity, proportionality, that only the information needed for a police investigation is obtained under the warrant, that this information is kept only for the time necessary for the investigation, and so forth.

The basic principles of necessity and proportionality seem appropriate to me. How do we articulate this as specifically as possible in the laws that empower judges to authorize the police to access certain information? I do not have a specific recommendation for you. Clearly, we are talking about provisions of the Criminal Code pertaining to orders to keep or produce information. First, the current criteria require court intervention, which is a good thing. Secondly, the criteria are rather lenient. I think we should question whether judges should be empowered, based on the case before them, to give the police the authorization requested and to set conditions to protect privacy.

Should metadata be defined in the Privacy Act? That would be helpful.

Is it in the Privacy Act? We know that the collection, use and sharing of metadata is not authorized under general privacy legislation alone. We would have to find a way to ensure that the definition and the rules surrounding collection, use and sharing—which is the crux of the matter—apply in all cases where such information is used.

I am not pleading here for standardized rules. I recognize that these activities depend on the context. The collection of data for the purpose of identifying risks to national security, the work of the CSE, the Communications Security Establishment, is one context, and the work of the police in a criminal investigation is another context where protections are generally higher.

● (1220)

That said, the applicable rules should certainly be indicated, in a general way. Moreover, the applicable rules should depend on the context.

The Vice-Chair (Mr. Joël Lightbound): In one of your recommendations, you say that the government should consult you before it implements laws or regulations that have an impact on privacy.

Do you think that your recommendations, further to this consultation, should be made public?

Mr. Daniel Therrien: Absolutely.

I think we should intervene as early as possible, specifically to reduce risks to privacy. Such a system must not, however, create the impression that the OPC is advising the party in power in one way and advising the other political parties differently. In exercising this responsibility, it is extremely important for us to be seen as acting impartially.

● (1225)

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

That is the end of my questions and of our meeting, Mr. Therrien, Ms. Lajoie and Ms. Kosseim.

We will suspend now and resume in camera to discuss committee business.

Thank you again for appearing before the committee.

[*Proceedings continue in camera*.]