HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 026 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, October 4, 2016

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, October 4, 2016

● (1105)

[*English*]

The Chair (Mr. Blaine Calkins (Red Deer—Lacombe, CPC)): Good morning, everyone.

We are resuming our study of the Privacy Act. This is our 26th meeting of this committee.

We're pleased to have joining us by video conference today some faces that we've seen at this committee before when we were doing the review of access to information. I'm pleased to welcome back Donovan Molloy, privacy commissioner; and Sean Murray, executive director from the House of Assembly in St. John's, Newfoundland and Labrador. Thank you very much.

We also have Catherine Tully, who is the information and privacy commissioner for Nova Scotia; and Drew McArthur, who is the acting commissioner from British Columbia.

B.C. is not online yet. Hopefully, Drew can join us as we start your presentation.

The way we have done this in the past is that we start with opening comments for up to about 10 minutes just in the order that you appear on the agenda.

Either of you from Newfoundland and Labrador can get us started, and we'll move to Catherine after that.

Mr. Donovan Molloy (Privacy Commissioner, House of Assembly, Office of the Information and Privacy Commissioner of Newfoundland and Labrador): Good morning.

We really appreciate this opportunity, Mr. Murray and I, to appear before you. We know you've already heard from the statutory review committee: Clyde Wells, Doug Letto, and Jennifer Stoddart. They certainly addressed the rationale for the recent changes in Newfoundland and Labrador with respect to our access and privacy legislation.

I've been commissioner for just over three months now, and as a newcomer to access and privacy, I find it quite remarkable how the ability in our present society to collect, analyze, and unfortunately, abuse information has grown dramatically and continues to grow. However, I was surprised to learn that the federal Privacy Act had not really been amended for over 30 years.

The situation that we're in now in the digital age is that, formerly, being secure in your home and being secure in your life meant basically that your home was your castle, and now, with the proliferation of information, its storage, and its use, the keys to that castle exist out there in the digital world, and you can be deprived of your privacy and sense of well-being without anybody coming through your door. It's vitally important that all government institutions collect only that information that is necessary and then do their utmost to safeguard that from inappropriate uses and from being accessed by sources outside of government.

We are in a very enviable position here in Newfoundland and Labrador because of the Access to Information and Protection of Privacy Act, 2015. We believe it's one of the best pieces of legislation in the country. However, we recognize that the solutions we are using here and that were implemented here may not apply universally, and perhaps, in particular, may not apply to the federal system. Issues of volume and resources may dictate or require different solutions.

As an example, in regard to mandatory reporting of privacy breaches, we have all breaches reported to us, not just material breaches. However, again, based on our volume of reports, that may be more practical in a jurisdiction such as ours and less practical with an institution the size of the federal government.

The recommendations that have been made by the federal commissioner in terms of necessity for collection, public education, and public research mandate are all, we think, extremely positive. For the most part, I think we support all of the recommendations that have been made by the federal Privacy Commissioner.

We believe that our experience, in terms of now having had over a year to deal with our new legislation and responses to it and accumulate data, may be of some benefit to the committee. Between ourselves, Mr. Murray and I, we will hopefully answer any questions you have today to the best of our ability.

Thank you.

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

Now we move to Catherine, for up to 10 minutes, please. Ms. Tully.

Ms. Catherine Tully (Information and Privacy Commissioner for Nova Scotia, Office of the Information and Privacy Commissioner of Nova Scotia): Thank you.

I haven't appeared before this committee before, so I thought I'd give you a bit of my background, which might give you some idea of the kinds of questions I might be good at answering for you.

I've been practising in the area of access and privacy law for 15 years. I've worked inside government. I administered the ATI, the access to information and privacy program, for the attorney general, the solicitor general, and the aboriginal relations departments in British Columbia for six years. My shop processed about 2,000 to 3,000 requests a year and we produced hundreds of privacy impact assessments. We administered the act inside a government department.

Then I switched to the oversight agency in British Columbia, where I was assistant privacy commissioner. In that capacity, my group of investigators and mediators investigated hundreds of privacy breaches and remediated thousands of complaints about access to information. British Columbia has an order-making power, so the small percentage of files that didn't settle moved over into the adjudication unit. So I'm familiar with that model of oversight.

I then spent a couple of years at Canada Post administering access and privacy on behalf of that federal institution under the Privacy Act and the Access to Information Act as the director of access and privacy. Now here I am in Nova Scotia, as the information and privacy commissioner. This is a recommendation-making authority in the province, so I've been inside and outside order-making and recommendation-making regimes.

I think you've heard from many people about the need to modernize the Privacy Act. In fact, I share the same concerns in terms of what's happening here in Nova Scotia. I'm in the process of developing a series of recommendations to modernize Nova Scotia's law, which was last significantly amended in 1993. It's 10 years newer but shares a lot of the shortcomings of the Privacy Act.

In preparation for this hearing, I looked at the submissions of my colleague Commissioner Therrien and I can say honestly that pretty much everything he is suggesting to your committee will be things that I'm suggesting to the legislature here in Nova Scotia. There's certainly a consistency in terms of where we see the need for these types of laws to go to be effective.

I thought I'd make three suggestions to you by way of introductory comments.

First, I would recommend that you try as best you can to make your changes as consistent as possible with private sector privacy standards, because from the citizens' perspective, what they don't get is that there would be different rules for the government as opposed to business. Often they find that the rules that businesses follow make more sense to them.

In terms of things such as collection of personal information, I know Commissioner Therrien recommended that you add a requirement of necessity. That's absolutely what's expected in the private sector. It makes perfect sense, of course, in the public sector and is a common standard across other jurisdictions, just not under the Privacy Act.

My second suggestion is that you consider adding a detailed purpose clause. I make that recommendation because Nova Scotia has a detailed purpose clause. It's one of the best parts of our old law. It's a very rich purpose clause and has served the courts well in their interpretation of the act. It has given a really good indication of what the legislature intended with the access to information and protection of privacy act here in Nova Scotia.

The third recommendation I would make to you has to do with breach reporting. Nova Scotia has a unique breach reporting requirement under the Personal Health Information Act. There is no breach reporting requirement under our old Freedom of Information and Protection of Privacy Act, but under the Personal Health Information Act, health custodians have to report minor breaches to my office. Real risk of significant harm or material breaches that you talk about at the federal level only require a notification to affected individuals, so I'm certainly recommending to the legislature that it include a notification of material breaches, much like Commissioner Therrien is recommending to you. I would also suggest that it would be worthwhile to require that institutions keep a list of all breaches, basically a privacy breach log.

That is something that the Europeans have done in the general data protection regulation in Europe. They must keep a log of all privacy breaches and keep it available should the commissioner wish to see it, and they must further report material breaches to the data protection authorities in Europe.

That seems to me to make sense, and I'll tell you why. Just looking at these minor breaches gives you an idea of what's going on and where the risks to personal health information are.

● (1110)

In Nova Scotia, for example, we had a 75% increase in minor breaches last year by health custodians. The patterns are really quite troubling. They give you very good intelligence about where training is required and where technical solutions are required in order to prevent the minor breaches, but also to prevent potential major breaches.

Those are three ideas that I thought I would suggest by way of introduction. I'm happy to address any other issues or any questions you might have.

● (1115)

The Chair: Thank you very much, Ms. Tully.

We still don't have our friends from British Columbia online, so I think we'll proceed with our rounds of questions. If we do get Mr. McArthur in from B.C., we will immediately move to his opening comments and then resume with our questions.

If that's all right with you, colleagues, we'll start our seven-minute round with Mr. Erskine-Smith.

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

My first question is with respect to order-making powers. I understand there's a hybrid model in Newfoundland. With respect to the order-making powers that you've experienced, Ms. Tully, can you speak to how formal the process tends to be as to whether it's a full tribunal hearing, and to what procedural fairness we're actually looking at if we're looking at an order-making model?

Ms. Catherine Tully: My experience with this was back in B.C., and it compared to what's happening in Nova Scotia with the recommendations.

When matters reached the stage where it went to adjudication, there was a wall between the informal mediation and the adjudication. It was quite formal relative to recommendation-making. Parties tended to be represented by lawyers. They provided witness submissions. There was an exchange of submissions. The hearings generally, though, almost exclusively, were in writing before a single adjudicator, but it required the B.C. office to have a group of adjudicators separate from the rest of the staff who conducted these hearings and issued written reports.

On the recommendations in my jurisdiction now, what happens is that there is no separation between the initial informal resolution process and the recommendation reports that I write, so parties don't need to have a lawyer but the quality of the submissions then is reflected in that they are not generally that strong and there's a lack of evidence. It's quite a challenge to write these recommendations.

Mr. Nathaniel Erskine-Smith: I see.

Moving to requiring consultation on legislation with implications for privacy, I note that it is in the legislation in Newfoundland. I think it's in section 112 of the act. Could you speak to your experience with requiring consultation, how often it's happened, and whether you would recommend that we adopt that provision?

Ms. Catherine Tully: I'm sorry, but are you asking me?

Mr. Nathaniel Erskine-Smith: No. It's for the commissioner from Newfoundland.

Mr. Sean Murray (Executive Director, House of Assembly, Office of the Information and Privacy Commissioner of Newfoundland and Labrador): I'm going to answer that one.

We are strongly in favour of section 112 of the act. We think it has worked out very well. We have been consulted a number of times since June 2015, when the ATIP of 2015 came in. We have provided input on draft bills and had an impact on the bill that was eventually tabled in the House of Assembly for debate.

Prior to that, there was an ad hoc occasional practice of consulting the commissioner's office. It was unsatisfactory because there were times when bills went before the House that we had not had notice of and were not aware of and that had a significant impact on privacy and access to information. There was a lost opportunity, then, to have that input. We think section 112 has been very helpful.

Mr. Nathaniel Erskine-Smith: Perhaps you could also speak to section 72, which requires privacy impact assessments.

Also, Ms. Tully, Mr. Molloy, and Mr. Murray, perhaps you could speak to whether we ought to incorporate such a requirement and whether, in your view, there's a difference between incorporating it in legislation versus in the rules that we have with the Treasury Board.

Mr. Sean Murray: I can address that from the point of view of Newfoundland and Labrador.

The privacy impact assessment requirement in our ATIP of 2015 was a new requirement. It is limited in that the privacy impact assessment is only required to be provided to the commissioner's office for review in the case of “a common or integrated program”. Unfortunately, there's been some disagreement between us and the government on the definition of “common or integrated program”, so we haven't seen too many for review.

However, there is still a requirement that public bodies complete a privacy impact assessment or a preliminary privacy impact assessment and provide it to the minister. We believe that has been a useful process in order for public bodies to get a good handle on the risks to privacy and to be able to address or mitigate those risks. Certainly, that's going to help with better privacy compliance for all those programs and initiatives that are subject to it.

● (1120)

Mr. Nathaniel Erskine-Smith: My last question is with respect to secondary use. You spoke to the importance of a necessity requirement for collection. Once government has collected that information.... Witnesses last week talked about different standards, so obviously in the private sector it's a consistent-use standard, with the initial consent that's been granted. In the public sector, you could have a consistent-use standard for secondary use, you could have a compatibility standard, or you could simply have a necessity and proportionality requirement for a further program.

I wonder if you could speak to rules in your jurisdictions with respect to further secondary use and what standard you think should be adopted.

Ms. Catherine Tully: I can speak to it from Nova Scotia's perspective, and actually across those three jurisdictions I've worked in.

I'm a fan of consistent use. I think the tests set out in the laws tend to define either consistent or compatible, and those rules are helpful in allowing for secondary use in those limited circumstances. That gives the definition "incorporates necessity and proportionality" in some of those pieces of legislation. Certainly, trying to be as consistent as possible with secondary use across the two, PIPEDA and the Privacy Act, would be helpful.

I've applied the consistent-use test and found it really works well for secondary use.

Mr. Nathaniel Erskine-Smith: Any comments, Mr. Molloy or Mr. Murray?

Mr. Sean Murray: I think Ms. Tully has captured it nicely.

Mr. Nathaniel Erskine-Smith: To push back a little bit, I wonder if the government collects information.... The example I used last week was collecting information at the border in terms of individuals leaving the country and how long they're out of the country. If that information is then to be shared with other departments to assess whether individuals can claim certain benefits, or not claim certain benefits because they've been out of the country too long, I wonder if we're talking consistent use there, or if there's a worry with that kind of sharing of information. If we have a test similar to the Oakes test, where it's a pressing and substantial government objective and the sharing of information is necessary and proportionate to that objective, and the salutary benefits outweigh the costs, should we be concerned about that secondary information sharing?

Ms. Catherine Tully: From my perspective, that is not a use question; it's a disclosure question. If it's across two separate institutions, they would have to satisfy the disclosure requirement, so they'd first have to have an authority. The idea of also layering on top of that for any disclosure a consideration of proportionality and necessity, I think, is a very good idea and speaks to.... Those provisions tend to be discretionary provisions, so giving some guidance in terms of, even if you have the authority, what you should consider in exercising your discretion, especially sharing between government departments, would be an excellent idea.

The Chair: We're well beyond the seven minutes for Mr. Erskine-Smith.

Before we move to Mr. Jeneroux, we have the folks from B.C. on the phone at least. It looks as though we're only going to get Mr. McArthur via voice only. We're not going to get video.

Mr. McArthur, you're going to have to fight your way into this from time to time, because we won't have any visual cues from you when you want to speak or answer a question.

I remind all of our witnesses that when you're having a conversation, and if somebody else is speaking, we can hear you. If you have a mute button at your disposal, or something like that, it would be handy to use.

We're going to move now to Mr. McArthur. Thank you for joining us. Sorry for the technical problems.

Is this Bradley?

Mr. Drew McArthur (Acting Commissioner, Office of the Information and Privacy Commissioner of British Columbia): This is Drew McArthur and Bradley Weldon.

The Chair: Thank you very much.

We have Mr. McArthur and Mr. Weldon from British Columbia.

We'll give you up to 10 minutes to make your opening remarks, then we'll go to the questions. Go ahead, please.

● (1125)

Mr. Drew McArthur: Thank you very much for the invitation.

My office provides independent oversight and enforcement over B.C.'s access and privacy laws. The enforcement and oversight extends to over 2,900 public bodies, including ministries, local governments, schools, crown corporations, hospitals, municipal police forces, and more. They're subject to B.C.'s public sector privacy law, the Freedom of Information and Protection of Privacy Act or FIPPA.

It extends to over 380,000 private sector organizations, including businesses, charities, associations, trade unions, trusts, and more that are subject to B.C.'s Personal Information Protection Act or PIPA.

Today I am going to focus my comments on three areas that are part of the deliberations of this committee to which the B.C. experience may be informative: commissioners order-making powers, an explicit obligation to safeguard personal information, and mandatory breach notification. Under order-making power and mediation and consultation, in British Columbia the mandate of the office includes the promotion of access and privacy rights, public education, advice to public bodies and businesses, investigation of complaints, mediation, and independent adjudication. These functions are complementary, and in my opinion, best delivered under one roof. It would be extremely difficult for another administrative tribunal or court to attain the same level of expertise and provide for efficient and timely resolutions for citizens.

Privacy and access to information issues are dynamic in the modern digital world. It's in the interests of organizations, individuals, and public bodies that the individuals making legal and binding decisions have the requisite skills and up-to-date knowledge about what is happening on the ground. Having the responsibility for adjudication plus advocacy, education, and investigation ensures the necessary expertise in the law. Our adjudicators receive the same technical training and professional development as our investigators, and are routinely exposed to new technologies, emerging ideas, and global trends affecting privacy and access to information law.

Combining the investigation and adjudication into one office provides clear benefits to citizens. Combining those provides one-stop shopping for citizens. This clarity and convenience is important. There is no confusion about which oversight agency or tribunal citizens need to direct their complaint to. They need merely to address our office. Citizens don't feel as though they are caught in or bounced around an unnecessarily bureaucratic system.

We have not found that the public education or the advisory functions of a commissioner pose a risk of undermining the adjudicative function. We do take steps to protect the integrity of the adjudication process. For example, no information about investigative files or attempts at informal resolution are ever disclosed to the adjudicators. The adjudicators do not report to the same supervisor, and they are not located on the same floor as the investigators.

When providing the public with advice and consultation, we clarify that our view is based on the information provided at the time, and that it is not binding on the commissioner with respect to making a formal finding in the event that we receive a future complaint.

In our consultations, we communicate about general principles and recommend best practices without prejudging individual cases. We are able to perform these various roles effectively because our legislation also explicitly gives us these powers and spells them out in detail.

Adjudication enhances our ability to resolve issues through mediation. The adjudicative function lends greater authority to our investigators by focusing the minds of the parties, and it provides an incentive to both parties to avoid formal adjudication. As a result, we resolve 90% of our complaints and reviews in mediation. In the last year we had 1,056 complaints and requests for review, of which only 109 went to inquiry. Of those that went to inquiry, only a little over 1% were judicially reviewed.

The fact that we have public education and advisory functions, complemented by investigative powers, with the ultimate ability to order compliance through our adjudicative function, gives us a level of authority that can influence the public and the government. Without that complete suite of functions, we would not have that same level of influence.

● (1130)

B.C.'s public sector privacy law has an explicit requirement for public bodies to safeguard personal information. We consider this legislative requirement as being fundamental to a public body's responsibility for the personal information it collects from citizens. Given the negative repercussions that can occur to citizens in the event of a breach of their personal information, it's almost unbelievable that a privacy protection statute would not incorporate this requirement.

Section 30 of our act states:

> a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

Citizens rely on this section and expect that a public body is taking adequate measures to protect their personal information. It's the legislative requirement in most jurisdictions across Canada and internationally. Having this requirement in legislation is important from the perspective of public trust, as a clear and binding requirement on public bodies. It indicates the importance that governments place on this requirement.

While B.C.'s legislation does not explicitly address physical, organizational, and technological measures commensurate with the sensitivity of the data, our office has set out similar expectations in investigation reports and orders. In my view, placing this language explicitly in the legislation would be consistent with international standards regarding the protection of personal information.

Also, we have been clear that, as our province's regulator, we evaluate “reasonable security arrangements” on an objective basis, and that the determination of what is reasonable is contextual. The standard is not one of perfection but varies based on the sensitivity and the amount of personal information in question.

On breach notification, a privacy breach occurs when there is unauthorized access, collection, use, or disclosure of personal information. It is unauthorized if it occurs in contravention of one of our privacy laws. An important element of safeguarding personal information is ensuring that the privacy commissioner and affected individuals are notified when a privacy breach occurs.

Privacy breaches can carry significant costs. They put individuals at risk for identity theft and serious financial or reputational harms. They can also result in a loss of dignity and a loss of confidence in public bodies. We trust public bodies with some of our most sensitive and comprehensive personal information: social security records, tax data, health information, financial information, and the list goes on. We have no choice but to provide that information to the public bodies.

It seems every week that privacy breaches are reported in the media. We hear about laptops and portable storage devices being lost or stolen, human error resulting in disclosure, unauthorized access, or snooping as well as cyber-attacks.

Breach reporting in B.C. is currently voluntary in both the private and public sector. However, my office has recommended that it be made a mandatory requirement, and let me explain why. In British Columbia, we examined the government's privacy breach management process and we published those results in 2015. We learned that nearly 3,000 breaches were reported to government during the period of 2010 to 2013, but only 30 of those had been reported to my office. This told us that, under a voluntary reporting requirement, my office was receiving reports of only about 1% of all the breaches that occur within government ministries. Of those, the majority, 72%, were classified as "administrative errors". The breakdown of other types of breaches included unauthorized disclosures at 16%, lost or stolen at 4%, unauthorized access at 3%, and cyber-attacks or phishing at less than 1%.

It shows that it's important to set out a clear threshold where notification must occur. We don't want to hear about every breach, but we need to know about the important ones. In B.C., we have recommended that the threshold be where the breach would be reasonably expected to cause harm to an individual, or where the breach involves a large number of individuals.

● (1135)

Mandatory breach reporting to a privacy commissioner also means that the commissioner's office can work with public bodies to learn from their mistakes and implement lasting preventative strategies. Mandatory breach notification also ensures that affected individuals are made aware of breaches without unreasonable delay, so they can take the important steps to protect themselves.

For these reasons, my office has recommended to the legislative committees reviewing B.C.'s privacy statutes that mandatory breach notification be added as a requirement. Both of these committees agreed and recommended in their final reports that the privacy laws for the public and the private sectors be amended to require breach notification to the commissioner and to affected individuals in the event of a privacy breach. The B.C. government has stated that it is committed to addressing mandatory breach notification at the next available legislative opportunity.

The federal Bill S-4 added breach notification requirements to Canada's private sector privacy law, and it is difficult for me to understand why the government would not hold itself to the same standard as it holds the private sector.

That concludes my remarks.

The Chair: Thank you very much. That was you, Mr. McArthur. Is that correct?

Mr. Drew McArthur: That is correct.

The Chair: Mr. McArthur and Mr. Weldon, for the benefit of our recording process here in Ottawa, please identify yourself at the start of any comments either of you make, so we can make sure that we attribute the comments to the appropriate person. We can't see who's talking, so that would be helpful to us.

Colleagues, I will ask you to be specific if you're asking a question of a witness to make sure they are clearly identified. If you're asking it of all witnesses, then I'll make sure that we get that through.

We're going to resume with our seven-minute round, and we'll go to Mr. Kelly for up to seven minutes, please.

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

I'd like each witness to give a brief statement—and we had a bit of that from B.C.—and describe a little about the nature of the types of privacy breaches you receive. We're talking about mandatory reporting, and the number of breaches could be quite high, at least based on the B.C. experience of an estimate of around 1% of the current breaches being reported. If all breaches are to be reported, a privacy breach can be any of a number of things, from the careless leaving behind of a piece of paper to a sophisticated cyber-attack, or a lost laptop containing thousands or maybe even millions of different records.

More specifically in the way that specific lives might be affected by such breaches, could each of you give a quick, even anecdotal, discussion of the kinds of things we're dealing with? I'll start with our Newfoundland and Labrador witnesses, Mr. Molloy and Mr. Murray.

Mr. Donovan Molloy: For the most part, the majority of the breaches reported to us—and we have mandatory reporting of all breaches under ATIPPA—are incidental, accidental, careless, and generally things that don't involve an intent to abuse, share, or disclose somebody's personal information.

We do have a number of instances where people have deliberately accessed other people's personal information and that has been shared or disclosed. The impact on the people who are affected by it is profound. Once you've been deprived of your sense of privacy and your dignity, depending on the nature of the information, it makes it difficult to move forward in your relationship with a particular public body or a government in general.

Conversely, we would note that we've experienced situations where the unnecessary notification of individuals that their privacy has been breached can cause a lot of damage, as well. Once you've been notified it's hard to put the genie back in the bottle. People have a hard job being convinced that the breach didn't have any impact on them.

● (1140)

Ms. Catherine Tully: In Nova Scotia, we do not have mandatory breach notification for significant breaches. Instead, what we see are the minor breaches I mentioned. I think we received reports of in the neighbourhood of 900 minor breaches of personal health information last year. About a third of those are missent faxes or the high-tech version of that, which is selecting the wrong provider code in a database so that health information goes to the wrong provider. It's these types of breaches that tend not to cause significant harm. Occasionally, we hear about more significant breaches. These are the snooping in databases. In small communities, that's quite significant both in terms of finding locations for individuals or finding medical information, including mental health information, which is quite embarrassing.

Mr. Drew McArthur: I mentioned briefly the kinds of breaches that we've seen in government. I'd like to highlight a couple that resulted in investigations. One was with the University of Victoria and involved an unencrypted hard drive containing employee personal information. The other was with our Ministry of Education and also involved an unencrypted hard drive. Although it was lost, it contained student data for over 300,000 students in B.C. These are serious circumstances where people may need to take action.

I'd like to add a further note on the need for thresholds in reporting. We have identified that the threshold in the public sector is when a breach could be reasonably expected to cause harm to an individual or if it involves a large number of individuals. We've set that for the notification of the commissioner, and when notifying individuals, we've recommended that the threshold be when it's expected to cause significant harm to the individual. Again, significant harm is contextual. We don't have experience with it yet. We've set the two thresholds to be slightly different in that a lower threshold for reporting to the commissioner would allow us to work with public bodies to make sure they have programs in place to prevent disclosure of this information to the unauthorized access user. It would also ensure that individuals are informed without unreasonable delay so that they may protect themselves.

Mr. Pat Kelly: What additional infrastructure would need to be in place to adopt mandatory reporting?

I understand that in Newfoundland and Labrador there is already mandatory reporting. Given the limited amount of reporting currently going on where reporting is not mandatory, what additional infrastructure would the federal government likely need to have in place, also noting that federal institutions are, in many cases, quite different from provincial institutions? Provincial institutions tend to be more service-oriented, where there are agencies with which people have a mandatory relationship like the CRA or the Canada Border Services Agency.

I'll let maybe each of you have just a quick moment to comment on what changes will need to happen within federal institutions to accommodate mandatory reporting.

The Chair: We're already past seven minutes, but if somebody has a quick comment on this, we'll get to it.

Mr. McArthur?

Mr. Drew McArthur: In terms of infrastructure from a technical perspective, nothing is required. It's merely a process to receive the complaints. I would note that in B.C., even though it is not mandatory, we already do receive, track, and investigate, if required, voluntary reports. We have the administrative processes established already. I also know that the federal privacy office has the process in place for receiving reports because I made those, unfortunately, from time to time when I was in the private sector.

● (1145)

The Chair: We're going to have to move on now. We're approaching eight minutes.

Mr. Dusseault, you have up to seven minutes, please.

[*Translation*]

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

My first question concerns an aspect that was mentioned by our friends from Newfoundland and Labrador concerning the mandatory regime that exists in that province. The provincial government is required to report to the commissioner when there has been a breach of privacy.

If you discover that that requirement has not been met and that the department has not reported the breach, does that result in consequences? Is the matter followed up? What happens when there has been a breach of privacy that was not reported to you?

[*English*]

Mr. Sean Murray: I don't think we've had the circumstance where there's been a breach that turned out to be something notable that wasn't reported to our office. You're correct that there are no penalties built into the act in cases where a public body fails to report a breach to our office. I guess that might be worth considering. We've had this for about a year and a half now, our new law, and we have noted that some public bodies seem to be reporting more breaches than others. It's something that we have inquired about, and I would suspect it's something we will probably follow up on in due course, but at this point I can't conclude that any public body has been purposely not reporting breaches to us. I guess that's something we'll have to look into.

[*Translation*]

Mr. Pierre-Luc Dusseault: Thank you.

I would like to go back to the witness from British Columbia regarding the requirement to inform citizens when their privacy has been breached. I would like to go back to what you also mentioned, that is to say the reputational harms, financial harms and even those concerning people's identities.

In British Columbia, is there a way for citizens to sue the government, for damages or even remedial measures? The Canadian commissioner is proposing remedial measures, including damages, for privacy breaches. Is it possible for a citizen in British Columbia to take legal action to obtain compensation?

[*English*]

Mr. Drew McArthur: At this point in time we're still awaiting the legislation to determine how it will actually be implemented. However, what we can do is order a public body to take the appropriate steps to mitigate the harm. In some cases that mitigation may involve credit monitoring or other steps depending on the circumstances.

[*Translation*]

Mr. Pierre-Luc Dusseault: Thank you, that is very interesting. It is nevertheless a measure the government can take in the circumstances.

Now I will speak to the commissioner from Nova Scotia, and this could be of interest to the other provinces.

I wonder whether an effort is being made to educate not only the population in this regard—which is very laudable—but especially government employees. The latter must know their obligations under the Privacy Act. They must be informed about what they do every day and what might have an impact on the privacy of the citizens of their province or Canada. Are security measures being put in place, for example, to inform employees about whether spam is being circulated? Are there any measures to inform government employees that they should not open certain emails and in order to prevent citizen privacy breaches?

[*English*]

Ms. Catherine Tully: As the information and privacy commissioner I do have an education mandate, but the government itself also has a central group who manages access in privacy, and they provide privacy training within the government departments proper. Most of the training that I do is for the smaller public bodies, the municipalities and the agency boards and commissions, because they have no other source of training. I have a bunch of tools available, including security standards and recommendations for steps to be taken. I have tools on how to manage a privacy breach. We offer privacy breach training to any public body, including government departments. We just completed that training. I know the government does send out these warnings about spam. The IT group central within government sends out regular kinds of warnings about activities to avoid. That's certainly happening at the government level, but privacy awareness is a big issue and one that requires quite a bit of training.

● (1150)

[*Translation*]

Mr. Pierre-Luc Dusseault: Since I have a little time left, I would also like to talk about certain provinces that may not have a law covering a large number of government institutions or organizations.

I wonder whether some of you can comment on the possibility of expanding the Privacy Act so that it applies to crown corporations, for example, and to other public organizations subject to certain federal statutes. I want to know your opinion on that and to hear some examples, if possible.

I believe a large number of organizations in British Columbia are subject to the act. First I would like to hear the comments of the commissioner from that province. What organizations are subject to that act? Do they include crown corporations and businesses and all public and even para-public organizations?

[*English*]

Mr. Drew McArthur: As I noted in my opening comments, the oversight in the public sector in British Columbia extends to over 2,900 public bodies. Those include the central core operations of government, but they also include municipal governments, schools, crown corporations, hospitals, and municipal police forces. It has a pretty broad covering.

I will note that there is an area that is not covered currently, and we have made recommendations that it be amended. There are some organizations associated with public bodies. Typically they are associated with universities. They are companies that are created by universities, but they are not currently covered under the act, and we believe they should be. That's a gap in our law.

[*Translation*]

Mr. Pierre-Luc Dusseault: Madam—

[*English*]

The Chair: Sorry, Mr. Dusseault, we're done, but we will get back to that.

For Ms. Tully and the folks from Newfoundland and Labrador, if you have some comments on that, I'm sure you'll have an opportunity to have input on that.

Mr. Saini, go ahead for up to seven minutes, please.

Mr. Raj Saini (Kitchener Centre, Lib.): First of all, thank you very much to all of you for being here.

The question I have is kind of unique, because all three of you practise under different models. B.C. has the order-making powers; Nova Scotia has recommendation powers; and Newfoundland has a hybrid model.

All of you act as privacy and information commissioners, and as you know, in the federal government, the office for information and the office for privacy are separate. In March, the Privacy Commissioner made a submission requesting the hybrid-model types of powers, and this committee, in its review of the Access to Information Act, recommended the order-making powers for the Information Commissioner. The Privacy Commissioner, having heard that the Information Commissioner got full order-making powers, also requested full order-making powers.

If you could just imagine both of your offices being split, how would you balance that? Do you think it's necessary that both the office of the information commissioner and the office of the privacy commissioner have the same powers, or should they be different? This question is to all of you.

Mr. Donovan Molloy: I think it's difficult to speak to the circumstances of the federal Privacy Commissioner.

In terms of our own experience, it would not be practical, because we have limited resources. Splitting the office would, I think, result in us being unable to fully effect our mandate under ATIPPA.

The model we have, whereby we make a recommendation that can become an order if it's not appealed to the court within 10 days, is very effective. It places the burden on the public body. It also allows us to participate in the court hearing, which is invaluable, because we get to give our own objective perspective in court. Sometimes in the case of a person who doesn't have the resources to have their own counsel, that is really the only substantive quality argument the court hears, other than the arguments that are filed on behalf of the public body.

● (1155)

Ms. Catherine Tully: If I understood your question correctly, if I imagine my office split so that there's access and there's privacy, your question is whether they have the same oversight authorities.

Mr. Raj Saini: Yes.

Ms. Catherine Tully: My view very strongly at the federal level, having been there, and thinking of it in the Nova Scotia context, is that the two offices are regulating the same entities. I would think it would be very important that they have the same authorities, either order-making or not, because day to day you're dealing with these two oversight agencies. I think it would undermine the authority of one if the other had order-making authority and it didn't, so I can see the practical reasons why they should be the same. Certainly, from my perspective as an oversight agency, I would want consistency across those two roles.

Mr. Drew McArthur: Our experience in B.C., of course, is having access to information and protection of privacy in a single statute with the order-making powers.

I can't tell you what it would be like to have two separate agencies, but in our case we have a holistic view of the operations of government from both perspectives and we can ensure that the appropriate recommendations are made, and in the case when we need it, we have the ability to implement orders.

Mr. Raj Saini: Do you think it would be ideal, then, to have both offices in one?

Mr. Drew McArthur: From our perspective, we've never experienced having the two separate. Just from the work we do, there are often cases where there are access to information and privacy issues involved in the same investigation. Our people have expertise on both sides.

Mr. Raj Saini: Is there anyone else?

Ms. Catherine Tully: I agree with Drew.

At the provincial level, it works really well, because this is the system we're used to. At the federal level, though, these are two huge issues and they take a lot of attention. It seems to have worked well having them separate. Those are my thoughts.

The Chair: I think our friends from Newfoundland and Labrador are trying to communicate with us, but they're muted.

Mr. Sean Murray: We are not muted here.

At the national level, especially, I think it's important to have a champion for access to information and a champion for privacy, who can be recognized and speak to those issues separately, be leaders across the country, and represent those issues internationally as well. I think it has worked very well from that perspective to have them as separate offices. At the provincial level, functionally, I don't think there would be any need to have that separation.

Mr. Raj Saini: The second question I have is about the potential pitfalls of the over-sharing of data. We've heard some concerns from other witnesses that, with data now moving from paper-based to digital-based, sometimes there can be an over-collection of data but also an over-sharing of data, not only within government but with other jurisdictions. One of the ways this has been solved in the private sector is by an opt-in, opt-out model.

Can you highlight how we can balance the government's requirement or need to operate effectively with making sure there is no over-sharing of data?

Mr. Drew McArthur: My initial response to that question is that there is a threshold in our provincial legislation that the data must be necessary for the operation of a program.

The inclusion of the word “necessary” in our legislation [*Technical difficulty—Editor*] the amount of over-collection and therefore protects from over-sharing in the after sense. The inclusion of “necessary” covers off the concern about whether information may be over-shared in one sense. In the other sense, in our case, we do have in our legislation the requirement for information sharing agreements, which would typically make the process transparent or —in the case of information that is sensitive for national security—at least ensure that the appropriate protective measures are being implemented when information sharing agreements are put in place.

● (1200)

The Chair: That takes us to the end of the seven-minute round.

Thank you very much, Mr. Saini.

We now move to the five-minute round, and we'll begin with Mr. Jeneroux.

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Thank you very much.

Thank you to all three of the groups for being here with us today on video conference. I appreciate your taking the time out of your day.

Before I move on to my questions, I think Mr. Saini let you off the hook a little too easy there, with some of those answers in terms of combining the offices. If I remember, Ms. Tully, you said the issues are important at the federal level. Are they not as important at the provincial level?

You folks in Newfoundland mentioned champions. Is that not championing at the provincial level as well?

Mr. McArthur, I think you said you don't know any other way, so it works.

Maybe you could elaborate on your positions just slightly. The other argument to that is cost-savings, if you combine the two, and that didn't come up in any of the answers. If you guys don't mind elaborating, before I get to my question, that would be great.

Mr. Drew McArthur: I think the only thing that comes to mind is that the size of our operation in British Columbia is approximately 40 people. That is not a large operation when considered against the size of the federal Privacy Commissioner's office or the Information Commissioner's office. There may be opportunities of scale, but in our case, because of our size and our jurisdiction, it remains effective for us having both access to information and privacy in one piece of legislation.

In some cases in the international context, the two are separated. It may make a difference when you're dealing with issues internationally.

Ms. Catherine Tully: I think the only other thing I would add is that the issues on the privacy side are complicated. The technology issues associated with it, the fact that data is moving around the world, these are all managed by these data protection offices that our Privacy Commissioner is an equivalent to. Having a leader in Canada on that issue I think is very important for our government and for the provinces as well. That stands out when you have an identifiable privacy commissioner and it's consistent with the approaches taken in other jurisdictions. I would say that it's likewise on the information side, having a leader in that way.

Mr. Matt Jeneroux: So you don't think having the minister of justice, which the Privacy Act falls under, would be enough of a voice internationally to do that.

Ms. Catherine Tully: I think those are very important voices, for sure, but there's a whole layer of these oversight agencies contributing significantly to the conversation around what our privacy standards are. Not only that, but they have these enforcement authorities, these fining authorities, that are making sure that these rules are followed. They're an important part. Both things have to exist, for sure.

The Chair: Mr. Molloy or Mr. Murray, did you have any comments on that?

Mr. Donovan Molloy: I don't think we're saying that they can't be done together and should never be done together. It's just that in certain circumstances it would seem better to have them apart. If you're talking economies of scale, when you go to, for example, order-making powers, then you're talking about expanding two offices.

It depends on where your values lie and to the extent that you have, in any given situation, a Cadillac or a Civic, I suppose.

● (1205)

Mr. Matt Jeneroux: Thank you. That's a great transition to my next question.

In terms of the order-making model, we've heard recently that a hybrid model is perhaps an option to move forward.

If we go around the group, we'll probably run out of time, but we can come back to it in my next line of questioning. What do you see works best, and what you would recommend as part of the Privacy Commissioner's recommendations?

Mr. Drew McArthur: In terms of an order-making power, as noted, we have that ability in our sector legislation. We have taken the opportunity to use that from time to time, and find it effective. It also, as we've indicated, turns the parties' minds, through the mediation process, to be much more in tune with the sensitivities of each party. It assists us in getting to the resolution of complaints at the mediation phase rather than having to proceed through, but it provides us with the ability for order-making powers should we have to go beyond the mediation phase or if mediation hasn't been accepted.

The Chair: That takes us to Mr. Long.

You have up to five minutes, please.

Mr. Wayne Long (Saint John—Rothesay, Lib.): Thank you, Mr. Chair.

Thank you to all our presenters this morning. I think this is very informative.

Mr. McArthur, I'm sorry we can't see you, but I've read a lot of your articles and I've read about you with great interest. You have a very interesting background. You were a founding member, I believe, of the Canadian Council of Chief Privacy Officers. You were chief compliance officer with Telus, and I believe the Telus privacy policy was actually a gold standard for policies like that.

Obviously you've worked in both the public sector and the private sector. I'm wondering if you could give us a comment on how working in especially the private sector maybe gives you a different perspective on things now that you're in the public sector.

Mr. Drew McArthur: In a recent presentation I made I highlighted some of the shifts in moving from being regulated to being a regulator. It's been an interesting learning curve for me and I've become more sensitive to some of the issues.

Specifically I'll talk about mandatory breach notification. When I was in the private sector, we worked very hard to come up with voluntary breach notification guidelines, and we worked with the privacy commissioners across the country to implement those as guidelines for organizations. I now see those embodied in the federal privacy legislation, Bill S-4. When the regulations are implemented, we will see that for federal private sector organizations. We see it in Alberta, and we've recommended it in B.C., and the B.C. government has accepted that.

What was once voluntary in the private sector is now becoming de facto standard of being mandatory. We also note that in Europe the general data protection authority has come out to indicate that mandatory breach notification is required. I'll also note that they've taken a few steps further than that, and it's going to be significant for Canada to continue to be substantially similar with the requirements of GDPR for the free flow of information as it relates in the private sector for organizations that operate multinationally.

Mr. Wayne Long: Thank you for that.

Mr. McArthur, I'm just going to stick with you briefly, then we'll go to our other presenters. I just want to get your perspective on the triple-delete scandal that happened in B.C., and the other one I read about was that there was a breach with Island Health. There was a chief of staff of the government who was basically charged. Correct me if I'm wrong, but he was really charged with lying to cover it up, not actually the delete, delete, delete. For those who aren't aware, they deleted them out of their inbox, then deleted them out of the trash file, and then deleted them off the server. I know you were quoted, saying, “There should be penalties and fines”. You feel they should be reprimanded more strongly. I just want to get your perspective on the triple delete, and then get our other panellists' perspective on the harshness of fines.

● (1210)

Mr. Drew McArthur: I will say the triple-delete investigation—we call it a scandal here in B.C.—resulted in a significant number of recommendations for government and a catalyst for change, so there has been some good coming out of that investigation. On the specific circumstances around the individual, you are correct in that he perjured himself in his testimony given to my former colleague Elizabeth Denham, the then privacy commissioner, and he was charged under the act. That was the first circumstance where that had occurred.

We have recommended that the fines to individuals be increased to a substantial level, and the reason for that recommendation is evident in some of the more recent, as the media calls them, snooping incidents into personal health records of individuals, where employees of health authorities who have access to patient information, but no need or business need to access specific patient files, go in and snoop. We believe there are significant deterrents required in order to prevent the amount of snooping that we see going on, not only in B.C. but across the country.

Mr. Wayne Long: Quickly, I know you said fines should be increased to a significant level. Correct me if I'm wrong, are they currently $5,000 for a breach?

Mr. Drew McArthur: Correct. We recommended to our committee that they be increased to $50,000, and the committee recommended to the legislature that they be increased to $25,000.

Mr. Wayne Long: Did you say $25,000?

Mr. Drew McArthur: That's correct.

The Chair: Mr. Long, I know you wanted to hear from others, but we are well past the five-minute mark so we're going to go back to Mr. Jeneroux. Keep in mind, colleagues, that we will have a bit of time at the end of the meeting. If you have some unfinished business or unanswered questions that you'd like to get on the record, we can certainly get to that.

Mr. Jeneroux, we're back to you for five minutes.

Mr. Matt Jeneroux: Wonderful. Thank you, guys. If we could follow-up with Ms. Tully, Mr. Molloy, and Mr. Murray on which model you would prefer, that would be great.

Ms. Catherine Tully: Is that a question going back to the order-making versus hybrid?

Mr. Matt Jeneroux: Yes. I'm sorry. To clarify, we have a number of models before us, one that the Privacy Commissioner prefers. What are your comments on what you feel is the best model that we should implement at the federal level?

Ms. Catherine Tully: From having experience with both order-making and recommendation-making, I can say without hesitation that plain recommendation-making is not a good model. I would say one of the other two is definitely what I would strongly recommend. As I have mentioned, I think consistency across those two offices is very important.

Order-making worked really well in B.C., I thought, for a lot of the reasons Drew has mentioned. When there's order-making, the informal resolutions go faster, the public body is taken more seriously, there's less foot-dragging, they're more willing to engage and engage quickly, and they have better submissions.

When you only get to recommend at the end, there's a degree of inconsistency in terms of who's accepting and who's not, so it's hard to set a good standard across all public bodies, because some are willing to follow the recommendations and some aren't. It definitely needs more.

I like the hybrid model for a small jurisdiction. I think that would really work. My office is very small. There are only seven of us. There's no way we're going to have resources to be able to have a separate adjudication unit, whereas the federal offices are large and probably much more capable of absorbing that responsibility.

Mr. Donovan Molloy: A pure recommendation model is completely ineffectual. From our point of view, the fact that a recommendation can become an order in 10 days motivates the public bodies and other authorities to co-operate and to get these things concluded, because if it goes to a formal report and they're not prepared to follow the recommendation, they have to go to court and they have to justify why they didn't. I think the hybrid model is fairly powerful as well.

● (1215)

Mr. Pat Kelly: Mr. Chair, if I may, I'm going to finish Mr. Jeneroux's time, if that's all right.

I'm going to pick up on something that Mr. Molloy mentioned. I think it was in response to Mr. Erskine-Smith's question or maybe it was in your opening remarks. You mentioned situations where reporting may compound harm done in a privacy breach, if I understood correctly.

Could you maybe elaborate on some of the perils of reporting where, yes, somebody's privacy may have been breached? Perhaps they had not come to harm as a result, and yet the reporting process may create harm.

Mr. Donovan Molloy: There's a tendency to err on the side of caution with respect to the notification of individuals. We certainly don't want to discourage notification, but the issue becomes the appropriate interpretation of what is a material breach, and secondarily, whether it is something that has the potential to harm someone.

If you have a breach, and you decide you're going to notify people that there has been a breach and they're at risk of harm, if they were never really at risk of harm, the individual notifications shouldn't have gone out. Then they come to our office, and we try and tell them that, no, this was a circumstance where we concluded that there was no risk of harm to you. Once you've been told that you've been put at risk by a breach of your privacy, it's very hard to convince anybody that they aren't at risk and that the notification was unnecessary.

People get stressed and they start worrying about identity theft, embarrassment in their community, and all kinds of things that they were never put at risk of having happen to them.

Mr. Pat Kelly: Thank you.

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

We'll now move to our last five-minute questioner.

Mr. Bratina.

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

I believe I heard that both the Newfoundland and Nova Scotia witnesses generally agreed with the recommendations that were put forward.

I'm wondering, Mr. McArthur, if you've had an opportunity to review the recommendations and whether you have a general opinion.

Mr. Drew McArthur: I have had an opportunity to review. In the areas that affect British Columbia, in the areas that I spoke about—those being mandatory breach reporting, order-making powers, and the requirement for safeguarding personal information—those were the general areas where we saw we could provide some insight as it relates to the operations here in British Columbia.

On a broader note, I really would only comment that it's been a significant number of years since the Privacy Act was amended. It probably is very timely and opportune that at this point in time you take the opportunity to bring it into alignment with the other activities that are going on around the country and internationally. There's been significant progress. I mentioned the general data protection regulations in Europe.

I'd like to give Bradley a moment to make a comment, as well.

The Chair: Mr. Weldon.

Mr. Bradley Weldon (Senior Policy Analyst, Office of the Information and Privacy Commissioner of British Columbia): This is Brad Weldon.

My observation here would simply be that our act is reviewed every six years, and every six years we have significant revisions recommended. I think it makes a lot more sense that our act provide for that sort of a review. It is, I think, remarkable that it's been this long since significant changes have been made to the Privacy Act.

Mr. Bob Bratina: Let me go on.

The Privacy Commissioner has recommended to "Grant the Privacy Commissioner discretion to publicly report on government privacy issues when in the public interest". I'm curious about that, because the Privacy Commissioner does have the power to issue special reports. These are typically annual reports to Parliament.

Perhaps I'll direct this first to Newfoundland and Labrador, but with the awareness that the Privacy Commissioner can make comments throughout the year at his discretion, I wonder whether there would be pressure on him, almost every day or week, to come up with media responses to any number of issues. Do you see any danger in that?

● (1220)

Mr. Donovan Molloy: Personally, no. The opportunity to make comments generally and educate the public is encompassed within our mandate for advocacy and public education. There are things.... For example, last week was Right to Know Week. I made some public comments about open government, open contracting. We're trying to educate people on how the system could work better.

There is really no need to go looking for an opportunity to do an individual report, unless something specifically of consequence has happened. We'd be very reluctant to start making it a weekly bulletin with "here's the latest". I think it would genuinely have to have merit, it would be significantly evaluated, and the public interest would actually have to require it as opposed to, maybe, favour it.

Mr. Bob Bratina: Ms. Tully, the recommendations include extending "coverage to all government institutions, including Ministers' Offices and the Prime Minister's Office, and extend rights of access to foreign nationals". On this recommendation, is your premier covered under this in the manner that the Prime Minister would be?

Ms. Catherine Tully: Yes. The offices of ministers are covered as the head of the public body.

Mr. Bob Bratina: Does that function well, in your view, in your experience?

Ms. Catherine Tully: There are some challenges with that, for sure, but I think it's a very important part of access law.

Mr. Drew McArthur: In B.C., the legislation does cover government and ministers' offices. There is an exception for cabinet confidences and a number of other exceptions. The threshold is pretty high over when government can withhold information, but it does apply to all the operations of government.

Mr. Bob Bratina: Thank you.

The Chair: Our last question is for Mr. Dusseault, for up to three minutes, please.

Does anybody else want to get their name on the list? Okay, I have Mr. Lightbound.

Monsieur Dusseault, please.

[*Translation*]

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

I am going to come back to the aspect that was just raised by Mr. Bratina, that is the commissioner's recommendation that the scope of the act be expanded so that it can be applied to ministers' offices and to that of the prime minister.

In Canada, it used to be enough to access the prime minister's website for our email addresses and certain other information to be requested from us. The Government of Canada gathers information. In fact, not only the government but, in some instances, ministers offices and the office of the prime minister do it as well.

Is the premier's office subject to the Privacy Act in your provinces?

My question is first for the representative from Newfoundland and Labrador.

[*English*]

Mr. Donovan Molloy: In Newfoundland and Labrador, the premier and all the ministers are subject to the privacy legislation.

[*Translation*]

Mr. Pierre-Luc Dusseault: What is the situation in Nova Scotia in this regard?

[*English*]

Ms. Catherine Tully: The same thing is true in Nova Scotia.

[*Translation*]

Mr. Pierre-Luc Dusseault: What about British Columbia?

[*English*]

Mr. Drew McArthur: Yes.

[*Translation*]

Mr. Pierre-Luc Dusseault: All right.

I have another question on the possibility of expanding the scope of the act.

Are political parties covered by the act? At the federal level, more particularly, we know that political parties often find themselves in a kind of limbo where they are not considered public entities or, more obviously, private businesses.

What is your experience in this area in your respective provinces regarding the situation of political parties, more specifically under your privacy acts?

I will begin with the representative from Newfoundland and Labrador.

[*English*]

Mr. Donovan Molloy: Political parties are not public bodies. They're not subject to the act.

[*Translation*]

Mr. Pierre-Luc Dusseault: Are they subject to provisions respecting private businesses?

● (1225)

[*English*]

Mr. Donovan Molloy: I hadn't really....

Mr. Sean Murray: Not to my knowledge.

Mr. Donovan Molloy: Not to our knowledge, no.

[*Translation*]

Mr. Pierre-Luc Dusseault: Is the situation the same in Nova Scotia?

[*English*]

Ms. Catherine Tully: It is the same.

[*Translation*]

Mr. Pierre-Luc Dusseault: What is the situation in British Columbia in this regard?

[*English*]

Mr. Drew McArthur: In British Columbia, all political parties—federal, provincial, and municipal—are covered under B.C.'s private sector privacy legislation, PIPA.

[*Translation*]

Mr. Pierre-Luc Dusseault: Thank you.

It is interesting to note that there may be a difference among the provinces on this point.

As my time is nearly up, I would like to go back to the role you play within the departments and public organizations to verify the level of protection that exists for personal information.

Are you directly involved in risk assessment? We know that risks are increasing these days, in this technological era. Are you involved yourselves, as commissioners, in assessing the risks of data theft or citizen privacy breaches?

How does that work in British Columbia?

[*English*]

Mr. Drew McArthur: In British Columbia, there are several ways in which we consult with government.

First, we are actually consulted when draft legislation is being considered to ensure privacy protections are included. Second, when governments are implementing new programs, we are also consulted. In some cases, privacy impact assessments are required, and we work with the government in understanding and mitigating the risks associated with that. Finally, in our legislation, we have the ability to audit. We have used that ability to go in and examine an operation to determine if the protections in place and the processes are considered best practice.

The Chair: That takes us to our free time, colleagues. We don't have anything else on the agenda, but I know that Mr. Lightbound would like to ask a few questions. If any of you have any other supplementary questions you would like to ask....

I then want a few minutes at the end, if you don't mind, to talk about the witness lists that are coming up for the remainder of the study.

Mr. Lightbound.

[*Translation*]

Mr. Joël Lightbound (Louis-Hébert, Lib.): Thank you, Mr. Chair.

First of all, I want to thank the witnesses for their contribution to this discussion.

My first question concerns one of the recommendations that Commissioner Therrien made, that he would like the information-sharing among government institutions and agencies to be governed by information-sharing agreements and accords that are detailed and public. I would like to know whether you have those kinds of agreements in your respective provinces on information-sharing among government institutions and whether they are public.

[*English*]

Mr. Drew McArthur: We do have in our legislation the requirement to create and implement "information sharing agreements" in accordance with the directions of the minister responsible for our act. These directions actually have yet to be issued, but so far the government is [*Technical difficulty—Editor*] guidelines on what information should be in an information sharing agreement and when an information sharing agreement should be completed.

We believe they're a useful tool to ensure compliance with privacy legislation. They document responsibilities for each of the parties to the agreement and the conditions around the collection and disclosure of personal information. We see them as a good measure for accountability when increasing amounts of information are being shared.

[*Translation*]

Mr. Joël Lightbound: Thank you.

Would the Information and Privacy Commissioner of Nova Scotia like to add something on the subject?

[*English*]

Ms. Catherine Tully: I was used to the regime that Drew has just described in British Columbia. Then I came to Nova Scotia where there's no mandatory requirement for information sharing agreements. There's no direction specific from government that's regularly followed, as far as I know, because there's no mandatory consultation with my office so I don't see them. I'm a big fan of information sharing agreements. It forces organizations and government departments to think about what they're going to share, why they're going to share it, what their authority is, and what security they're going to build around it. It's a very good tool. It tends to make them reduce what they're doing, be clear why they're doing it, and monitor how it's happening.

● (1230)

Mr. Sean Murray: If I can speak from our perspective, we are in a similar situation to Commissioner Tully. We don't have a requirement under our legislation for information sharing agreements. I couldn't tell you the extent to which they're being employed. I believe that on an ad hoc basis they are being used from time to time, but we wouldn't have the opportunity to review them because it's not mandatory under our legislation.

We have, on occasion, recommended an information sharing agreement when we have had an opportunity to be involved. For example, we would recommend that type of thing when we're involved with conducting an audit or an investigation or if a public body comes to us seeking consultation voluntarily.

Mr. Joël Lightbound: If I may, I have just one last question for Madam Tully. I think it was in your opening statement that you mentioned something about the detailed purpose clause that you have in Nova Scotia. I was wondering if you could elaborate on what it entails.

Ms. Catherine Tully: Regarding the purpose clause in Nova Scotia, it's more on the access side in terms of how useful it's been, but I could see it working in a similar way on the privacy side. It spells out the series of things that are intended to be accomplished by the law, things like facilitating informed participation in policy formulation, ensuring fairness in government decision-making, and permitting the airing and reconciliation of divergent views.

It's interesting, when a legislature states these purposes so clearly, that when there's a possibility of interpretations of some of the sections, these purposes really guide the courts and the decision-makers. This is a unique opportunity for your committee and Parliament to anticipate some things and put some sign posts out there for the future because, of course, it takes some doing to amend these laws.

[*Translation*]

Mr. Joël Lightbound: All right.

Thank you very much.

[*English*]

The Chair: Colleagues, that brings to an end this particular discussion with our esteemed panellists, our guests here today. Thank you, Mr. Molloy and Mr. Murray, for coming again. I know you were here at our previous study. Mr. McArthur and Mr. Weldon, it was a pleasure having you here. Apologies if anything on our end kept us from connecting on the video side of things, but we certainly appreciated your testimony. Of course, Ms. Tully, we appreciate your perspectives, as well. I know that this will help us as we make recommendations and draft a final report. Hopefully, we will see some legislation in this Parliament that will address this antiquated legislation. I have every reason to believe that's going to happen.

Thank you again for your time and for your patience, and we know that we can count on you if we need further clarification. If there's anything else that you'd like to follow up with us on, please get it to the committee for consideration.

Colleagues, I have just a couple of housekeeping items. We have witnesses this Thursday. We have Chantal Bernier, who's a former privacy commissioner. Canada Revenue Agency and Shared Services Canada will also send folks in. On the Tuesday after we get back from Thanksgiving, we have CSIS, CBSA, and the RCMP. We're lining up witnesses for the 20th. We don't have confirmation from any of the ministers yet, but we're still working on that and waiting to hear back.

At some point in time, after we get back, I think we're going to have to have a discussion about what we're going to do next. I know there's a motion on the floor to propose what we're going to do next, but we need to have that discussion, as well.

I'm just going to let the committee know that I've already spoken to Mr. Lightbound, who will chair the meeting on Thursday. I have to go back to Alberta for some personal business that I need to attend to on Thursday, so I appreciate that. I know you're in good hands.

That brings me to the point where I wish you all a happy Thanksgiving, and I hope you have a safe constituency week. I look forward to seeing you in the House for the next couple of days, but I will be returning back to Alberta tomorrow night.

Does anyone have any questions or comments or anything they want to bring to the committee's attention?

Mr. Jeneroux.

Mr. Matt Jeneroux: We recently received an order in council from Ms. Chagger, Leader of the Government in the House of Commons, regarding the appointments of the Ethics Commissioner and the Lobbying Commissioner. I have a copy here if you would like to see it, Mr. Chair. It's a normal order in council.

I thought it might not be a bad idea, if the committee agrees, to call in the Ethics Commissioner and the Commissioner of Lobbying —I think they have been appointed for six months—to get a sense of what they plan to do. It might be the last opportunity to call in Ms. Dawson before she retires as well.

I don't know if we need a motion for that or just a general discussion.

● (1235)

The Chair: It is something this committee has done in the past.

Mr. Dusseault, you are the former chair of this committee. As a matter of protocol, when the committee had these orders in council, did it usually take the opportunity to have them come in and appear?

[*Translation*]

Mr. Pierre-Luc Dusseault: It was really at the committee's discretion. It was up to us to decide whether to invite newly appointed persons to appear before the Standing Committee on Access to Information, Privacy and Ethics in order to ask them questions about their mandate.

In this case, we are dealing with six-month term extensions. These persons occupy positions on an interim basis. I do not know whether it is necessary to invite them to appear in this instance. However, it is up to the committee to decide the matter.

[*English*]

The Chair: I don't think Mr. Jeneroux has actually put a formal motion here. I think he's asking if the committee is interested in entertaining and hearing from both Ms. Shepherd and Ms. Dawson in their reappointments; they were only six-month extensions, I think.

Mr. Lightbound.

[*Translation*]

Mr. Joël Lightbound: Would it not be better to invite them to appear toward the end of their terms which would enable us to gather their impressions as they prepare to leave their positions? They still have six months remaining. This is only a suggestion I am making. I think it would be interesting to invite them to hear their recommendations at that time.

[*English*]

Mr. Matt Jeneroux: My feelings aren't going to be hurt if we do it at the beginning or at the end.

I agree that there's probably a benefit to having them here, especially with everything we've discussed. I think the last time they were here, we were all pretty green on the committee as well, so I wouldn't mind taking an hour closer to the end.

Does it say when their end date is? Are we looking at March?

The Chair: I have the order in council appointment. There was another piece of paper that dealt with the actual term. I remember seeing it. I believe both of them were six-month extensions.

Does anybody else on the committee remember reading that? I don't want to have to dig it up.

[*Translation*]

Mr. Pierre-Luc Dusseault: We will also have to verify whether there is a limited period within which to invite commissioners to discuss their appointments. It might be interesting to hear from them around the end of their terms, but to do so before the new commissioners arrive. It would no doubt be interesting to know how their term went and to ask them questions about the future challenges they foresee.

Later on, once the permanent appointments have been made, it will be particularly appropriate to invite the new commissioners to hear about their vision for the future and the way they expect to carry out their respective terms.

[*English*]

The Chair: The appointments were made at the end of July for six months. Was that for Ms. Dawson, or was that for Ms. Shepherd ?

The Clerk of the Committee (Mr. Hugues La Rue): That was Ms. Dawson.

Mr. Matt Jeneroux: Again, Mr. Chair, there might, for example, be a 30-day time limit in terms of inviting them. If we can invite them and have them appear by the end of their term, I'd be okay with that. I just want to make sure we're in line with that 30 days.

The Chair: I need to be clear, Mr. Jeneroux, on what your intent is. If the intent is to scrutinize or to discuss the order in council, in that case we should do it sooner rather than later, or is your intention, as a matter of courtesy, to hear from them at the end of their term? I'm seeking some clarification from you, sir.

Mr. Matt Jeneroux: I guess we could do both. I'd be happy to do both.

The Chair: It's just that it doesn't make any sense to scrutinize the appointment of the order in council, after the order in council has already been executed.

Mr. Matt Jeneroux: I'm not complaining about the order in council. It's a six-month appointment. It makes sense to me. I would love to just hear their thoughts on where they plan to take the position and what they think should be changed about the position going forward, if they are not to have another extension as in the case of the Commissioner of Lobbying.

● (1240)

The Chair: Both of them received six-month extensions roughly at the end of June or early July, which means they're already halfway through their six-month term. We only have about half their time from those extensions remaining.

I think it's a matter of courtesy, and I don't see any dissenting opinions on this. It would be nice to maybe have them give us a state of the union address for their respective—

Mr. Raj Saini: Basically, you're asking for an exit interview, right?

Mr. Matt Jeneroux: Yes.

Mr. Raj Saini: You want to know what their experiences were and what they can recommend to.... That's fine.

The Chair: We want to know where things are right now.

Raj, are you okay with that?

Mr. Raj Saini: Yes, that's fine

The Chair: Okay, so we'll just have a gentlemen's agreement at the table that we'll pursue that.

Mr. Matt Jeneroux: I will invite them.

The Chair: Thank you very much.

Thank you, colleagues.

Have a happy Thanksgiving, and we'll see you in a couple of weeks.

The meeting is adjourned.

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

SPEAKER'S PERMISSION

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 Parliament of Canada Web Site at the following address: http://www.parl.gc.ca

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

PERMISSION DU PRÉSIDENT

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.

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 du Parlement du Canada à l'adresse suivante : http://www.parl.gc.ca