HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Industry, Science and Technology

INDU • NUMBER 036 • 2nd SESSION • 41st PARLIAMENT

EVIDENCE

Tuesday, March 10, 2015

Chair

Mr. David Sweet

Standing Committee on Industry, Science and Technology

Tuesday, March 10, 2015

● (1105)

[*English*]

The Chair (Mr. David Sweet (Ancaster—Dundas—Flamborough—Westdale, CPC)): Good morning, ladies and gentlemen. *Bonjour à tous*.

Welcome to the 36th meeting of the Standing Committee on Industry, Science and Technology. We are studying Bill S-4, an act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another act.

We have before us today, from the BC Freedom of Information and Privacy Association, Vincent Gogolek, the executive director.

We were going to have the Insurance Bureau of Canada here, but they're stuck on the tarmac in Toronto in a plane that was not able to go. They're trying to get on another plane, but of course they're not going to be able to make it to the meeting. We have already rescheduled them by phone for another meeting.

We also have before us Michael Geist, Canada research chair in Internet and e-commerce law at the University of Ottawa. He is testifying as an individual.

By teleconference we have Philippa Lawson, barrister and solicitor. She's coming to us from Whitehorse in Yukon.

Can you hear us okay, Ms. Lawson?

Ms. Philippa Lawson (Barrister and Solicitor, As an Individual): Yes, I can, thank you. Good morning.

The Chair: Great. Good morning.

We'll go with the orders of the day in front of us. We'll begin with the opening remarks by Mr. Gogolek.

Mr. Vincent Gogolek (Executive Director, BC Freedom of Information and Privacy Association): Thank you, Mr. Chair.

Thank you, committee, for having us here.

You have our submission and there are a number of links in it to related documents. I won't take you through that. I'll just raise some of the points in there, and hopefully that will leave more time for questions on what is a very important piece of legislation.

I also want to say that we appreciate the fact that the committee is hearing from witnesses before second reading. We take this as a positive sign that the government is in favour of and open to amendments above and beyond its usual openness in the normal course of proceedings.

The first thing I'd like to talk about is the Spencer decision of the Supreme Court of Canada from last year. I'd like to concentrate on the B.C. aspect of it. As you know we have a special legislative committee that looked at our substantially similar legislation: the Personal Information Protection Act. The committee came out with recommendations for changes to our equivalent of section 7. You have the link to that report, I believe, through our submission.

The approach they suggested was a narrowing of the scope of the B.C. section.

The special legislative committee in B.C. also raised concerns—some of which we raised with them, as did the Information and Privacy Commissioner, Elizabeth Denham—about the question of substantial similarity between the provincial and federal acts, so there is some discussion in there.

In addition to the B.C. committee and the B.C. commissioner, the federal Privacy Commissioner, Mr. Therrien, has also indicated he has some concerns with section 7, and has suggested some changes.

The second point I'd like to make is something that we raised not before this committee, but before the access to information, privacy and ethics committee relating to political parties. Political parties are not covered at the federal level by privacy legislation. The large amounts of data collected by political parties are essentially unregulated. I don't think this is suitable. I don't think this is appropriate, and I think it diminishes the confidence that Canadians have both in the privacy law, because of this very large hole, but also in terms of what happens to their personal information.

I offer to you, by way of contrast, what we have in British Columbia where our provincial political parties are covered by the Personal Information Protection Act. Our commissioner has conducted investigations into complaints that were brought to her by individuals about the conduct of political parties. The commissioner investigated, reports were issued, and practices were changed, and yet the political system continues. There has not been a complete collapse of the political system or the political parties in British Columbia. I offer to you, as an example, what can be done and the kind of thing I think could be easily done by including the political parties under PIPEDA.

The final point—and I'll be quite brief because I believe that Ms. Lawson will be dealing with this as well—is a report we are currently working on for the federal Privacy Commissioner called "The Connected Car: Who is in the Driver's Seat?" The report will be released March 25 in Vancouver and we'll be happy to provide you with copies.

● (1110)

I'll leave Ms. Lawson to deal with some of the particulars. Of course we won't be revealing the report here today, but there are a number of issues related to privacy, of course, and consent and consumer choice. I think members of the committee will find that report very interesting, and we hope it will inform your work as well.

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

Mr. Geist, we will now turn to you for your opening remarks, please.

Dr. Michael Geist (Canada Research Chair, Internet and E-commerce Law, University of Ottawa, As an Individual): Thank you, Mr. Chair.

Good morning. My name is Michael Geist. I'm a law professor at the University of Ottawa, where I hold the Canada research chair in Internet and e-commerce law. I've appeared before this committee on a number of occasions on digital policy issues, including privacy, and I appear today, as always, in a personal capacity representing only my own views.

Actually I previously appeared before the Senate committee that was studying Bill S-4 and my remarks then focused on three broad issues.

First, I offered my support for several important provisions in the bill, particularly the additional clarification on the standard of consent, the extension of the deadline to take cases to the Federal Court, and the expansion of the powers of the Privacy Commissioner to publicly disclose information related to findings or other matters. Second, I identified issues that I think need amendment or improvement: the security breach disclosure rules, particularly the abandonment of a two-step disclosure process that was found in some earlier bills; the compliance agreements provisions, which I think could be strengthened with penalties or order-making power; and the expansion of voluntary disclosure of personal information between private sector organizations. Third, I talked about some missing provisions, namely, what I think is the need for mandatory transparency reporting.

My time this morning is limited, so I'm going to delve deeper into just two issues, the voluntary disclosure provision and transparency reporting.

On voluntary disclosure, as you know, Bill S-4 expands the possibility of personal information disclosure without consent or court oversight to anyone, not just law enforcement. As you know, the bill features a provision granting organizations the right to voluntarily disclose personal information without the knowledge or consent of the affected individual and without a court order to other non-law enforcement organizations provided they are investigating a breach of an agreement or legal violation, or even the prospect of a future violation.

This broadly worded exception will allow companies to disclose personal information to other companies or organizations without court approval. I believe this runs counter to the court decisions that we've seen from the Federal Court, which have sought to establish clear limits and oversight over such disclosures as well as the spirit of the Supreme Court of Canada's Spencer decision, which ruled that Canadians have a reasonable expectation of privacy with such information. In fact, if we examine the leading cases involving disclosure of customer information in private litigation—not to law enforcement but in private litigation—such as in Warman v. Fournier, BMG v. Doe, Voltage v. Doe—virtually all emphasized the need for safeguards before customer information is disclosed, even as part of an investigation.

A House of Commons committee did recommend a similar reform in 2006, but that recommendation was rejected at the time, both by the Conservative government and the Privacy Commissioner of Canada.

I recognize that some have suggested that both Alberta and B.C. have similar provisions and that no harm has resulted from their approach. I'm not so sure. I don't think anyone can reasonably conclude that the provincial approach has not resulted in privacy risks or harms. It's important to bear in mind that the disclosure itself is not necessarily revealed to the affected individual. Indeed, the point is often to disclose without knowledge or consent, meaning the affected individual will not know that their personal information has been disclosed. Asking for evidence of harm when the harmful conduct is kept secret from those who are affected creates an impossible evidentiary burden. In fact, even if you believe that the disclosures might come to light through court processes should it reach that point, and we know that oftentimes the disclosures won't ever reach the point of a court case, provincial privacy law such as we find in Alberta and B.C. rarely involves having these kinds of cases come to light. It's no coincidence that the leading cases involving personal information involve PIPEDA, because those cases typically involved telecom companies, Internet service providers, websites, and banks, all largely governed through PIPEDA.

In other words, the existence of this kind of provision at the provincial level actually tells us very little about how it will be used under PIPEDA. The reform here, I think, is clear. There is no compelling need for a change. The current system has been in place for many years and there are dozens of organizations that are covered by the investigative bodies exception. It may have been a bit of a hassle 10 years ago, but now the reform makes little sense. Further, if there are specific industries that can point to concerns, I think those can be addressed through a narrow amendment, but the broad provision that we have here opening the door to massive expansion of non-notified voluntary disclosure without any of the kinds of limitations that we typically find even the courts asking for should be removed.

Second is the need for transparency reporting. The lack of transparency in reporting requirements associated with personal information disclosures, I think, is a glaring omission from the bill. The revelations last year of over a million requests and over 750,000 disclosures of personal information in a single year, the majority of which happened without court oversight or a warrant, point to, I think, an enormously troubling weakness in Canada's privacy laws.

● (1115)

More recently, the Privacy Commissioner of Canada tried to conduct an audit of RCMP requests for subscriber information and was largely forced to abandon the audit when the data there were found to be inaccurate and incomplete.

Now, there are some companies, such as Rodgers and Telus, that have begun to issue transparency reports, but there are others, most notably Bell, that have not. Most Canadians have simply no awareness that this is taking place. This deficiency can be addressed, I think, through two reforms.

First, the law should require organizations to publicly report on the number of disclosures they make without knowledge or consent and without judicial warrants. This information should be disclosed in aggregate on a quarterly basis—every 90 days. I'm not talking about disclosing it to each individual immediately; we're talking about its being on an aggregate basis and a quarterly basis.

Second, those organizations should be at some point in time required to notify affected individuals within a reasonable time. Leave aside the necessity to keep it secret, if necessary as part of an investigation; once it is concluded or a reasonable amount of time has passed, either get a court order to continue the secrecy or disclose the disclosure to the affected individual.

The adoption of those kinds of provisions—transparency reporting and that disclosure—would, I think, be an important step forward in providing Canadians with greater transparency about the use and disclosure of their personal information.

I welcome your questions.

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

Now we'll go on to Ms. Lawson, who is joining us by phone.

Please go ahead with your opening remarks.

Ms. Philippa Lawson: Thank you very much.

Good morning, committee members. Thank you for the opportunity to address you on the matter of Bill S-4, which proposes amendments to PIPEDA.

My involvement with this legislation goes back to its genesis with the CSA model privacy code and the subsequent initiatives to legislate voluntary standards. As a lawyer with the Public Interest Advocacy Centre at the time, I was a public interest representative on the committee that drafted the code. I later advocated for legislation that eventually took the form of PIPEDA.

I have been closely involved with PIPEDA ever since, first in my role as a consumer advocate with PIAC and later as director of CIPPIC, both of whom I understand you have already heard from. In particular, I have conducted studies of private sector compliance with PIPEDA. I have lodged a number of PIPEDA complaints with the Privacy Commissioner. I have taken the Privacy Commissioner to court in order to establish that she had jurisdiction to enforce PIPEDA against foreign corporations acting in Canada. I published a study of security breach notification laws in 2007. I've been urging the government to adopt mandatory security breach notification laws since 2003.

Today I am speaking on my own behalf as a lawyer and privacy advocate. The last formal submissions I made on PIPEDA reform were in 2008 in my role as director of CIPPIC. Those submissions focused on three issues: security breach notification, protection of minors, and compliance and enforcement. The analysis and proposals made in those comments remain apt today, and I would be happy to provide copies of that submission to anyone who is interested.

I'm happy to see that the government has seen fit to address all three of these issues in Bill S-4, but I am disappointed that the measures in each case fall far short of what is needed. I will address each of these three topics briefly, but before doing so I would like to address an elephant in the room. That elephant is consent.

There is a pretense that companies are obtaining informed consent from customers to the collection, use, and sharing of their personal data. But anyone who takes the time to study what is actually going on will quickly see that this is, to a large extent, a fiction and that meaningful consent is rarely obtained from consumers.

Negative option consent is commonly used but rarely brought to the attention of customers. Consent is in fact often assumed simply by virtue of use of the service. Changes to privacy policies are simply posted on the company website and customers are expected to inform themselves. No one really expects individuals to read through lengthy, complex terms of service for every transaction. People simply don't have the time. If they do take the time to read the terms, they may find that they are notionally consenting to have their personal data used for purposes such as—and I'm quoting here from privacy policies that I've looked at—research, marketing, product development, and business purposes. In further violation of PIPEDA, many companies are refusing to deal with customers who won't agree to unnecessary uses of their personal data, such as marketing.

A reality check is needed on what is happening in the marketplace with so-called customer consent. In the meantime, proposed section 6.1 is a helpful qualification on what the law already requires. It may have some positive effect on what is, in my respectful submission, a widespread disgrace.

However, the current wording of proposed section 6.1 could actually have a perverse effect on the protection of children or seniors. If you read the clause, you will see that it fails to protect vulnerable populations to whom an organization's activities are not directed. All that a company needs to do to exploit children is to direct its activities to adults and then turn a blind eye to the fact that children are signing up. A simple fix is to revert to the earlier wording of this clause found in Bill C-12. However, if if the aim is to protect children, a much more effective approach is simply to prohibit certain uses of personal data about children.

● (1120)

I have a few words on breach notification. This is long overdue, and it will certainly be an improvement on the current situation. But are the proposed rules going to be effective? Breach notification is about more than notifying individuals. An equally important goal is to create incentives for organizations to put in place strong security safeguards.

In order to create such incentives, there needs to be a real risk of significant financial harm to a corporation from failing to put in place adequate security measures. This is the test you should be applying to your assessment of the proposed breach notification regime: is there a real risk of significant financial harm to corporations from non-compliance?

I am not convinced there is. Fines apply only to failure to report or failure to keep records and require cumbersome proceedings and proof of intent. Civil lawsuits are too costly to make sense in most cases, and the Privacy Commissioner may be dissuaded from using publicity for this purpose as a result of subsection 20(1.1), which prohibits disclosure of breach notification reports. I do not understand that section.

Until there are real financial incentives for corporations to take appropriate measures to prevent breaches from happening in the first place, and to otherwise comply with privacy laws, non-compliance with PIPEDA will continue to be a cost of doing business in Canada.

I'd like to finish with a few comments on private investigations. I am very concerned that, if the proposed changes to the current investigative body regime exception go through, this bill will actually set back privacy protection in Canada.

I will not repeat the able submissions of my colleague Dr. Geist on this subject, but let me just point out that in the new world of cheap data storage and powerful data analytics, the only limits on how far companies will go in their efforts to detect fraud, criticism, or contractual breaches will be what you put in this law. With today's technology, it's less costly to gather more data and to apply analytical tools to a large database than it is to restrict the intake of data to that needed in the first place.

In this context, insurance companies and other companies will, no doubt, argue that it's reasonable for them to conduct what amounts to broad and deep surveillance of their customers in order to detect fraud.

Paragraph 7(3)(d.2) would allow just that. It requires no formal investigation. The disclosure just needs to be reasonable, not even necessary as in the previous formulation in Bill C-12. This provision would open the door to routine sharing of personal data among organizations based on nothing more than the always present risk of fraud. Moreover, there would be no transparency or accountability requirements. It would be a major setback for consumer privacy.

I understand that this amendment was based on the Alberta model, but I looked at the Alberta model, and subsection 20(n) of the Alberta statute is not as permissive as this. It actually limits sharing to certain kinds of organizations.

I urge you to remove these clauses from the bill and stick with the current investigative body regime. I also urge you to adopt the transparency measures that my colleague Dr. Geist recommended.

Thank you very much.

● (1125)

The Chair: Thanks very much, Ms. Lawson.

We're going to go to rounds of questioning now. With a little math, and making up for the fact that sometimes even though I'm trying to keep very close to the time—it bleeds over a bit—we'll just do eight-minute rounds right across the room for each member.

We'll begin with Mr. Carmichael for eight minutes.

Mr. John Carmichael (Don Valley West, CPC): Thank you, Mr. Chair.

An eight-minute round seems like an eternity. It's a nice change.

Welcome to our witnesses. Good morning to all. Thank you for your testimony here today. It's good to see you all here.

Dr. Geist, thank you for your opening comments. There's a lot for consideration.

You suggested this bill may go too far in regard to changes around the investigative body regime. The Privacy Commissioner has suggested that there is no evidence from B.C. or Alberta that the system is actually flawed, and other stakeholders tend to support that amendment.

I wonder if you could respond to that.

Dr. Michael Geist: Sure. Just to reiterate some of the opening remarks that I made along those lines, I think we've actually seen a lot of people come forward and express concern about the particular provision. But specifically in regard to the Privacy Commissioner's comments—and I thought it was a good question—as I noted in my opening remarks, I frankly think it's almost an unfair burden to say where's the evidence of harm from Alberta and B.C. when people are kept in the dark about when these disclosures take place.

By definition, we are talking about disclosures that may occur where there is no notification of the person who's affected. We're talking about providing those kinds of disclosures without consent and without further disclosure. So these may well be happening, which I would argue in some instances may well be harmful, but frankly the affected individuals simply don't know. Therefore, I think it is very difficult to reach the conclusion that somehow this hasn't been harmful. These disclosures may well be happening under that regime—and indeed the way that Ms. Lawson described it, it seems somewhat likely that they are occurring—but most people won't even know this is happening. Moreover, if we look at the cases where these kinds of issues do come to light, which is typically when it finally makes it to court, they invariably involve Internet service providers, telecom companies, and the like, cases that go through PIPEDA. The notion that somehow we can get a good sense of what will happen under PIPEDA based on the experience in Alberta and B.C., I think is simply wrong because we don't even know what's really been happening in Alberta and B.C., and even if we did, we can see what takes place under PIPEDA, that being real efforts to try to get disclosure without appropriate oversight.

● (1130)

Mr. John Carmichael: Thank you.

You've been calling for mandatory data breach notifications and reporting on this for quite a period of time. Could you explain why you feel it's just that important to PIPEDA, and expand your thoughts on that at bit?

Dr. Michael Geist: Sorry, do you mean mandatory security breaches, or the transparency report?

Mr. John Carmichael: Let's go with transparency for starters.

Dr. Michael Geist: Sure, to start with transparency reporting, I think what we've learned over the last year is that privacy has become a major issue for many Canadians. It's the enormity of disclosures that are taking place without any sort of awareness. This is happening, frankly, I think to all of us. This is outside of Snowden-type revelations. It comes down to telecom companies and others being asked to disclose information on individuals hundreds of times every week. Up until fairly recently, we weren't even aware that was taking place.

One way to counter that is not to say that where there's appropriate investigations...and now, through the Spencer decision, appropriate oversight, stopping that from taking place. I think Spencer makes it clear that we need to have court orders when that takes place. But what we need as well is the ability to understand at least in aggregate how this is taking place. Transparency reporting would achieve that.

What we've had so far in Canada is a bit of a mixed bag. We have had companies like Rogers and Telus providing reports, although they differ somewhat, but the largest company of all, Bell, is simply standing on the sidelines and not disclosing. I think there's a problem when you have millions of Canadian customers of a company like that who don't even know under what circumstances the company discloses this information, and how frequently they disclose it, oftentimes without court oversight. Mandatory transparency reporting would help fix that.

Mr. John Carmichael: Thank you.

Mr. Gogolek.

Mr. Vincent Gogolek: Yes, I'd like to just chip in here in terms of the B.C. situation. Our commissioner, Ms. Denham, in her submission to the special committee to review our PIPA on November 26, 2014, on page 21, noted the following:

> *Spencer* may have clarified the constitutionality of warrantless disclosures to police, but it did not do the same for disclosures between organizations. It is currently not possible for my Office or for the public to know how much personal information has been or is being disclosed without the knowledge or consent of individuals under section 18(1)(c).

That's the equivalent of section 7.

> For this reason, transparency reports should also include information about disclosures to other organizations.

The commissioner's approach was adopted by the special committee in B.C., and not only are they calling for transparency reports, they're also calling for them to be published—so, not secret reports but published reports.

Mr. John Carmichael: Just out of interest's sake, do you see the sheer volume of this reporting becoming a problem in terms of bottlenecks, that we'll be able to act on it? That's obviously the goal at the end of the day.

Dr. Michael Geist: We've seen a couple of the largest telecom companies in the country, such as Rogers and Telus, start to do it. We've seen smaller players like SaskTel and TekSavvy do it. I think it's clearly doable. We've seen larger players on the global stage that face far more complicated circumstances. Vodafone, for example, discloses this for 40-odd countries. The notion that a company like Bell can't, or more accurately, I think, won't, is a real problem. And, no, I don't see any significant challenge.

The real problem has been that so much of this has taken place under the radar screen. The point is that when you've got Privacy Commissioner auditors going into the RCMP and finding that their data is inaccurate and incomplete, that strikes me as an urgent problem that ought to be addressed.

Mr. John Carmichael: Thank you very much.

Ms. Lawson, I'd like to include you in this round, if I could.

You talked about the failure to report on keeping records. What impact do you think the new compliance agreements will have on the commissioner's ability to enforce compliance with PIPEDA?

● (1135)

Ms. Philippa Lawson: I think they will be helpful, for the reasons that the Privacy Commissioner has already expressed to you.

I don't think that compliance agreements go far enough, though, in terms of giving the Privacy Commissioner the powers he needs to enforce compliance with this legislation. I don't understand why we don't give our federal Privacy Commissioner the same order-making powers as those given to his provincial counterparts, who administer similar legislation at the provincial level.

Mr. John Carmichael: Good. Thank you.

You talked about proposed section 6.1 and you suggested that it's a helpful provision, Ms. Lawson, but one that may have some negative impact on seniors and children.

I wonder whether you could expand upon that. We've had quite a bit of discussion around this issue over the past number of meetings. Could you comment on it? When you talk about the disclosures of privacy and consent and then look at the complexity and length of those documents, how do you see us fixing that problem?

Ms. Philippa Lawson: Those are two questions. I'll address the first one, which is the specific one about proposed section 6.1.

I think the useful thing to do is compare the proposed wording that you have in front of you with the text that was in the previous version of this bill, Bill C-12. The version that you have has a new phrase inserted.

The old one said:

> the consent of an individual is only valid if it is reasonable to expect that the individual understands the nature, purpose and consequences.

The new one says:

> the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences.

First of all, changing “the individual” to “an individual” and then adding “to whom the organization's activities are directed” has now made it possible for organizations to simply direct their activities to the general adult population and not worry about the fact that children, seniors, or other vulnerable persons are notionally consenting to having their personal information used for things that they don't really understand.

The Chair: Thanks, Ms. Lawson. I allowed an extra minute there for you to complete your answer. We'll have to try to get the rest of your answer in in another round.

Ms. Borg.

[*Translation*]

Ms. Charmaine Borg (Terrebonne—Blainville, NDP): Thank you very much, Mr. Chair.

I would like to thank all of our witnesses for being here today. You all have some very interesting points of view.

My first question relates to the Spencer decision.

Mr. Geist, you have already testified before the Senate, but the decision had not yet been made. So I would like to hear your opinion on the decision and its possible repercussions on Bill S-4.

When the minister appeared, he seemed to think that no changes to Bill S-4 and the PIPEDA were required. I would appreciate hearing the other witnesses comments on this, if they have any.

[*English*]

Dr. Michael Geist: Sure. Thanks.

The Spencer decision, as I think we've all recognized and have seen raised now concerning a number of bills and committees, finally brought to a head a long-standing, simmering issue around the question of whether there was a reasonable expectation of privacy and subscriber information. The Supreme Court of Canada quite clearly left no doubt that there is.

Bill C-13, the lawful access bill, which of course has now been passed, and Bill S-4 were I believe both drafted at a time when there was some amount of uncertainty. Government in particular, I think, took the view that they could argue that there was not a reasonable expectation of privacy in that information and that, therefore, either warrantless disclosure or voluntary disclosure was consistent with the state of the law.

That uncertainty changed last June when the Supreme Court of Canada issued its Spencer decision. My view is that the spirit of that decision, which clearly recognizes that there is a reasonable expectation of privacy of the information...so much so that we now see law enforcement shifting towards a world that recognizes this point, and which has to obtain a warrant before they get the information. That recognition surely ought to be consistent with what we put in legislation within something such as Bill S-4.

The problem with Bill S-4, drafted before Spencer, is that it runs completely counter to it. The expansion of voluntary disclosure without condition, as many other courts in other kinds of cases have said, without court oversight to me appears to run directly against the spirit of Spencer.

While Spencer of course deals with a law enforcement situation and here we are dealing with a private sector situation, the information itself is the same. It's subscriber information, and the question is under what circumstances we disclose. Moving towards expanding that disclosure through voluntary measures runs directly counter to what I think the Supreme Court of Canada has identified as the appropriate standard for disclosure.

● (1140)

[*Translation*]

Mr. Vincent Gogolek: Given the complexity of the vocabulary used, I will answer in English if I may.

[*English*]

I agree with what Professor Geist has just said. The federal Privacy Commissioner has noted that there are difficulties with Bill S-4 as a result of the Spencer decision. Our commissioner in British Columbia has as well. Commissioner Denham has been calling for tightening of our legislation “without consent to cases where the disclosure is “necessary” for purposes related to an investigation or proceeding.” At the same time that the current version of Bill S-4 is taking one approach, one of the substantially similar provinces—one of the committees—is heading in the opposite direction as a result of their understanding and interpretation of the Spencer decision. As Professor Geist said, the drafters of Bill S-4 didn't have the advantage of Spencer. We do today. We know what the Supreme Court of Canada said about this. I think we have to take this into account.

[*Translation*]

Ms. Charmaine Borg: Thank you very much.

Mr. Gogolek, I would like go back to the Personal Information Protection and Electronic Documents Act, or PIPEDA.

You were actively involved in assessing this legislation following the Spencer decision. I read with great interest the report that was produced and that recommends amending the legislation to improve the framework for disclosing information without consent and without warrant.

Obviously, we do not want to establish 10 different privacy protection regimes in Canada. We want to ensure in some way that it is comprehensive.

If we are in the process of amending an act that Bill S-4 is supposed to resemble, should we not be proactive and amend the bill so that it corresponds to the new act?

Mr. Vincent Gogolek: It's more an issue of harmonization and, for that, there are two key factors to consider. The first is privacy protection of all Canadians. As you said, the fact that this protection varies from province to province is not a good thing. Why would British Columbians be better protected than Ontarians or Newfoundlanders? I don't think this is the approach we should adopt. I am convinced that it is your responsibility to make these acts similar overall. This concept of similarity is legislative.

Mr. Carmichael asked a question about this earlier.

[*English*]

As for there being different regimes—things that are not quite the same—this also deals with the compliance of organizations and companies. If companies have different requirements in different jurisdictions, having to do one thing in B.C. or Alberta or Quebec and then something else in the rest of Canada—which gets back to Ms. Lawson's comment about order-making power—they will decide that, well, we've been ordered to do something by the B.C. commissioner, so we have to comply with that or be in contempt of court. This is the good thing about the compliance agreements, but, ultimately, we need order-making power, because a company may decide that it doesn't want to do that. So we will end up in different situations.

● (1145)

[*Translation*]

Ms. Charmaine Borg: Thank you very much. I have one last question for you.

We are studying this bill before second reading, which is a rather unique situation. For me, this means that we have an opportunity to really improve the bill and make important amendments in order to properly protect the privacy of Canadians. We also have the opportunity to go beyond Bill S-4. We can adequately amend PIPEDA to properly protect Canadians.

Do you think that, in the wake of the Spencer decision, we should amend the provisions of PIPEDA that relate to the disclosure of information without consent? Should we go that far? Do you think it's necessary to do this? Should we take this opportunity?

My question is for all of the witnesses.

[*English*]

The Chair: We only have enough time for one answer.

Dr. Michael Geist: I'll jump in quickly by saying I think you raise a great point. Even today, I think we've already heard a bunch of potential suggestions about the kinds of things we could do that go beyond the four squares of the legislation itself.

With respect to Spencer, I think it points to what would be a really problematic outcome, one in which we find that where law enforcement is seeking information, they obtain court orders, whereas where that same information might well be disclosed in a private sector circumstance, there is no oversight or no limitations other than those found in the legislation. But as Ms. Lawson pointed out, they aren't very strong.

I think finding some amount of consistency, in terms of how we address the disclosure of personal information, especially when we're talking about things like subscriber information, which nowadays tells so much about our daily lives, would be very valuable and would allow us to have a more cohesive approach to privacy protection in Canada.

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

We will now move on to Mr. Daniel for eight minutes.

Mr. Joe Daniel (Don Valley East, CPC): Thank you, Mr. Chair, and thank you everybody who is here.

I'd like to direct my initial question to all of you, but we'll start with Ms. Lawson.

Ms. Lawson, in your introduction, you talked about defining when a breach should be reported by saying that it should be a real risk of significant financial loss. Can you perhaps expand on that a little bit? What would you consider to be significant financial loss?

Ms. Philippa Lawson: I was doing this bit of turn of phrase taking the legislation as it applies to security breach notification and applying it to companies. I think you need to step back, look at the big picture, and say, “Is this going to be effective? Are there sufficient incentives for industry to comply?”

When I say “comply”, I don't just mean reporting the breach and keeping the records of it; I mean complying by putting in place adequate security measures in the first place. I would think that what we're trying to do, first and foremost, is to make sure that companies put in place reasonable security safeguards. You need incentives for that, and in the private sector those need to be financial incentives.

I'm not sure if that was your question, but the point I was making is that I'm concerned that we may not have adequate incentives. A very strong incentive is negative publicity, and I don't understand why the Privacy Commissioner is being dissuaded in this legislation, under section 20, from publicizing those reports. Why don't we make them public? Why isn't transparency reporting part of transparency disclosure?

The submissions that CIPPIC made in 2008 on this issue were that we should establish a public registry of security breaches. Why are we treating these as confidential?

Mr. Joe Daniel: Thank you.

Mr. Geist.

Dr. Michael Geist: My concern with the security breach disclosure provisions, which I think quite clearly are long overdue —we've been passed by by so many other countries and jurisdictions on this—is frankly that we had it better in the earlier iterations of this bill, in Bill C-12 and Bill C-29, which, as I'm sure you know, created a two-step process.

The first step is notification to the Privacy Commissioner of a material breach, and that, of course, didn't include the necessity of the real risk of significant harm. It was more a matter of the breach itself.

Then you get into the secondary question of under what circumstances you go down the much more challenging avenue of having to disclose this breach to everyone who's affected, recognizing that there may be circumstances in which that's appropriate and others in which it's not.

What we've done here, by removing that and creating a higher threshold for all disclosures, I think means that systemic breaches don't get disclosed. It means that, many times, important material breaches simply don't get disclosed, and organizations that have underlying problems don't have to fess up at all.

I think we recognize that in some circumstances we have the incentives for organizations not to disclose because of the costs and the embarrassment factor. We also want to ensure that we don't have so many disclosures that consumers are receiving notifications on a daily basis, and they simply tune all of that out.

There is a balance to be struck, but I think we did a much better job, the government did a much better job, of striking that balance, particularly for things like systemic breaches within an organization, by saying, “Surely that's the sort of thing that we would want the Privacy Commissioner's office to know about”, and yet we've effectively removed that in this bill. It's hard to understand why.

● (1150)

Mr. Joe Daniel: Mr. Gogolek, do you have any comment?

Mr. Vincent Gogolek: I think I would just agree with the other two witnesses. I think it is important, as Professor Geist stated, as related also to the transparency reports and making them public rather than private, that we do know about this, especially in terms of, as Professor Geist just suggested, the commissioner being aware of situations where there could be a systemic problem. I think that's vital.

Mr. Joe Daniel: Thank you.

Following on from that, clearly the Internet doesn't have any borders as such. That adds a dimension of complexity towards privacy, breach of privacy, and things like that. In fact when we actually talk about all this reporting, in my view it doesn't necessarily capture the theft of data, which the organization may not actually even know, having seen lots of different ways of hacking computers, etc.

Does the mandatory data breach reporting help to reduce the risk of identity theft? Anyone can start.

Ms. Philippa Lawson: Absolutely; I would say that the first and foremost most important purpose of breach notification is to put in place incentives for the companies themselves to put in place the security measures that prevent the identity theft from happening in the first place.

But I'm concerned for the reasons I've expressed. I'm concerned that the regime here is not strong enough.

Mr. Joe Daniel: Okay.

Does anybody else want to comment on that?

Mr. Vincent Gogolek: Again, I'm agreeing with Ms. Lawson, but also, in terms of dealing with the question of breach notice fatigue, I think it's possible to deal with that through the notification itself. If it's something that does not relate to...or where you're just being advised that something happened that may affect your personal information, it's different from, “Okay, you'd better cancel your credit cards and get new ID”, or things like that.

So I think it can be dealt with at that stage rather than just saying there's no obligation to report.

Dr. Michael Geist: The answer, of course, is yes, security breach disclosure does help address identity theft, for the obvious reason that it creates a stronger incentive for organizations to do a better job of securing the information they collect. It provides notification to users in some circumstances so they can take appropriate safeguards and try to mitigate against the potential harm that could occur from identity theft. But let's be clear: we've waited nine years for this legislation. We started conducting hearings on this back in 2006. This is a long period of time. Merely saying that we have a provision that will help, but not help as much as we could otherwise....

Particularly given the kind of globalization of information that you've suggested, and particularly given, I think, our increasing awareness of the harm that can arise out of identity theft, we have to get it right. We don't just have to try to get a provision that will help. We have to get a provision that will in an optimal way ensure that Canadians are more effectively safeguarded against identity theft. As I've tried to suggest, I think we can do better.

● (1155)

Mr. Joe Daniel: Okay.

How much time do I have left?

The Chair: You have 20 seconds.

Mr. Joe Daniel: All right.

On the consent issue, I mean, nobody actually ever reads any of that consent stuff before they use some of these products. What suggestions do you have to improve that process?

Ms. Philippa Lawson: I would say to stop focusing on consent so much and put in place some hard limits. Let's acknowledge that consent is unrealistic in many situations, and put in place hard limits on what companies are allowed to collect in the first place and use and disclose later on.

The Chair: Thank you, Madam Lawson.

Ms. Sgro, you have eight minutes.

Hon. Judy Sgro (York West, Lib.): Thank you.

That's the area that I am most concerned about. Every time we pick up our BlackBerry or whatever gadgets we have, I agree that we don't read it. I would suggest that very few people read any of that. It's just an automatic check. It's a nuisance, and we just agree to it—until we find out that we have no protection, or very little protection. I think that's what we are trying to do here: to look at how to protect the consumer.

I attended a conference on cybersecurity yesterday. Certainly the issues that were raised there about security, whether you're talking about the Internet and so on, somehow make Bill S-4 look like it's still nowhere near what it should be, or the kind of legislation we need to be putting forward to better protect Canadians. I think it's unrealistic, frankly, to think that with this legislation companies are going to be reporting all of these breaches and so on. I think they'll ignore it. I think a $100,000 penalty is insufficient for a significant breach, based on the kinds of things we're learning through this process.

Certainly, Dr. Geist, your comments about transparency and disclosure would go toward improving it, as far as the real risk that consumers are facing is concerned, before they get into things like identity theft and violation of their basic rights. I don't want all my information shared with every Tom, Dick, and Harry who wants it. If we are going along with Bill S-4—and, from my party's perspective, I'm not sure that we are, but at least we're trying to make some improvements—what else would you suggest we need to put in here to make it stronger and more enforceable? I would ask that of all three, given my timelines here.

Dr. Michael Geist: Sure. Perhaps I'll start by highlighting a couple of things.

We've talked, obviously, about the security breach rules and about the voluntary disclosure, but focus for a moment on penalties and order-making power. I think that to an expert in privacy who came to Canada and learned that our federal commissioner does not have order-making power, that would be, frankly, stunning. His provincial counterparts have it. His counterparts around the world have it. Frankly, it's embarrassing for our federal commissioner to go to international meetings of other similarly placed data protection and privacy commissioners and find that he simply doesn't have order-making power as his counterparts do. To me, compliance agreements are a step in the right direction, but order-making power is actually the more appropriate solution.

With respect to penalties, I think you're right. I think tougher penalties do make a difference. If anything, the government has provided us with a good example of how that can happen: the anti-spam legislation, which of course is coming in for some amount of criticism, but I was a supporter of it. I was on the national task force that looked at this issue, and I appeared before a committee. I think one of the places where it gets it right is with tough penalties and a clear opt-in consent approach. It basically says that consent is a fiction at some point in time, but it's a particular fiction under PIPEDA. We somehow have reached the conclusion that things like negative option check boxes, the little boxes at the bottom of a web page that you're never quite sure if you're supposed to check or uncheck if you want to have your information used or not—it's oftentimes designed to be confusing—are appropriate as a standard of consent. That's bunk. I mean it's clearly not.

What CASL, the anti-spam legislation, tried to do, was up that with opt-in consent and real penalties. We saw the CRTC come forward with more than a million-dollar penalty against one organization just last week. Those are the kinds of penalties that get the attention of organizations. That's a higher standard with respect to consent that I think also clearly has an impact. In some ways we have a model—the government has passed it—with respect to commercial electronic marketing. What we need to do now is to take that sort of model and acknowledge that it ought to apply far more broadly with respect to privacy protection in the private sector.

● (1200)

Ms. Philippa Lawson: Perhaps I could jump in.

The Chair: Sure.

Hon. Judy Sgro: Go right ahead, Ms. Lawson.

Ms. Philippa Lawson: I have three points in answer to your question. I agree with everything Dr. Geist just said.

The first point is to put in place hard limits where we can. For example, when it comes to protecting children and seniors, just say in the act under subsection 5(3), which is already a hard limit but is vague, that it include no marketing of children or seniors; no collection, use, or disclosure of personal data of children and seniors for marketing purposes. That's already in the marketing industry's code of conduct. Put it in the legislation.

The second point is on real consent. As Dr. Geist said, forget this fiction of negative-option consent. Require express opt-in consent for all non-essential uses of customer data, including marketing. What I found in my research is that companies across the board are now including marketing as one of their primary purposes of collecting our data in order to provide the service we've asked them to provide. They are now treating marketing as a primary purpose. They're certainly not getting express consent. In many cases they're not even getting negative-option consent; they're not even letting us opt out of that.

The third point is on order-making powers. As Dr. Geist said, penalties should be easy to impose. Penalties should not require intent, proof of intent, and quasi-criminal proceedings, but should be administrative monetary penalties such as what the anti-spam law is using.

Hon. Judy Sgro: Mr. Gogolek.

Mr. Vincent Gogolek: Just to elaborate a little bit and maybe take it to a slightly different place and come back to some of the things we were talking about before, one of the advantages of having penalties is that penalties generally are reported: company X was fined by the Privacy Commissioner. It's not just the monetary hit, but the reputational hit. Companies that have bad practices and bad procedures will have to pay a price for it. They will pay the price in terms of the fine, but they will also have to pay a price in the marketplace. As for deals with the private sector, companies don't want to be obviously and consistently deficient in protecting the personal information of their customers.

Hon. Judy Sgro: I have one further question.

In your report, Mr. Gogolek, you mentioned bringing Canadian political parties under PIPEDA.

Would you like to elaborate a bit on that?

Mr. Vincent Gogolek: You are the politicians. You've presumably all used your various party data bases. You know that there's a lot of information collected on a lot of people. One of the problems is that parties are not subject to any restrictions on this. All the various penalties and protections we've been talking about here in terms of the private sector don't apply to political parties, at least not at the federal level.

Again, I would offer you the example of the situation in British Columbia, where the parties are subject to the act and where we have seen the process in action, with the commissioner conducting investigations and issuing reports as a result of complaints about how personal information was being dealt with or about party procedures. The parties have changed the way they deal with things and life goes on. I think everybody involved has a better feeling of how the system works. At least we know that there is some level of protection. If something goes wrong or we feel uncomfortable, we do have an avenue of redress, which doesn't exist right now at the federal level.

The Chair: Thank you.

And now we go to Mr. Warawa, for eight minutes.

Mr. Mark Warawa (Langley, CPC): Thank you, Chair.

Thank you to the witnesses here today.

I think each of the witnesses is aware that there have been hearings back to 2006, which I think Mr. Geist referred to.

PIPEDA was written in the 20th century. It's over a decade old and it needs to be improved. This is what Bill S-4 attempts to do.

Also, it is almost impossible to get unanimous support for any piece of legislation, so I think there has been a lot of energy that's gone into improving PIPEDA. Canadians want companies to tell them if their personal information has been lost or stolen and if they've been put at risk. I think that consent needs to be appropriate, particularly for target groups like children.

Dr. Geist, you've been involved with providing input to the Senate. You were involved in the hearings back in 2006.

My question is for Mr. Gogolek. When the Senate dealt with this at committee a year ago—not quite a year ago, but when the hearings at the committee in the Senate were beginning on Bill S-4, did you appear as a witness? As you're aware, any legislative changes have to be supported in both Houses, and Bill S-4 began in the Senate and is now in the House of Commons. Were you a witness when this was dealt with at the Senate?

● (1205)

Mr. Vincent Gogolek: No, I was not.

Mr. Mark Warawa: Did you provide a submission?

Mr. Vincent Gogolek: No, we did not.

Mr. Mark Warawa: Why not?

Mr. Vincent Gogolek: Well, we were not asked.

Mr. Mark Warawa: We do get submissions regularly presented to the chair, and this is a very important issue, and I welcome your input today, but again, any changes, amendments, would have to be agreed in both the Senate and the House, so if we were to make amendments now, after all this work, it would have to go back to the Senate. There is not adequate time for it to be passed in this Parliament.

Ms. Lawson, did you appear as a witness at the Senate?

Ms. Philippa Lawson: No, I did not. I was not invited and I did not appear or participate at the Senate stage.

However, I believe both CIPPIC and PIAC did, and they made a number of the same points that I'm making now. When I look back at the debates, many of these points were made at that stage, and I just don't understand why those amendments were not made by the Senate.

Mr. Mark Warawa: Did you provide a submission when this was dealt with at the Senate?

Ms. Philippa Lawson: No, I did not.

Mr. Mark Warawa: Okay.

Chair, I think it would have been very helpful if these points had been made at both the Senate and the House.

My question relates to a presentation made by the commissioner. The commissioner made a presentation not quite a year ago, in June of last year, before the Senate committee as they were dealing with Bill S-4, and then appeared before this committee on February 17.

I just want to read the summary of the commissioner. The commissioner does have new tools and greater flexibility to enforce PIPEDA. The commissioner said:

> Overall, the introduction of Bill S-4 is a positive development for privacy protection in Canada. PIPEDA was written in the 20th century. It is more than a decade old. From a privacy perspective, the world has changed dramatically during this relatively short time. Passing Bill S-4 with a few adjustments will strengthen PIPEDA and help the Office of the Privacy Commissioner better protect Canadians while addressing the emerging privacy issues of the 21st century.

Also unable to be with us today, Chair, is the Insurance Bureau of Canada. They provided a submission to the Senate when this was dealt with last year and they've communicated their support for aspects of the bill, particularly the fraud prevention measures.

Generally, the committee has heard support for this, and it's important that we provide the protection Canadians want. Bill S-4 does that.

Do any of the witnesses here today have a critique of the commissioner's perspective in supporting Bill S-4 going ahead?

● (1210)

Dr. Michael Geist: Sure. I'll do that. I'd also like to just note a couple of things. The commissioner did not appear before the Senate committee on Bill S-4. Because of the long delays in getting a commissioner appointed at that time, there was no commissioner, but people from that office were in a position to appear because it had been studied. So the commissioner actually didn't appear on Bill S-4.

In terms of lengthy study, with respect, let's be clear. The committee began a review of this bill in November 2006, and by May of 2007 it released its report.

We got first reading of Bill C-29 in May 2010. A second reading took until October. There were never any hearings held on Bill C-29.

The next bill that was introduced was Bill C-12, which was the second attempt at this bill. It sat at second reading for two years without moving forward. There were no committee hearings held on it.

We finally now have Bill S-4, on which there were two sets of hearings. Four days were allocated to this piece of legislation within the Senate: one day for the minister to appear; another day for clause-by-clause; two days for hearings. So if we're going to talk to witnesses about not having appeared, frankly, there were very, very few witnesses who had the opportunity to appear at all. This is, with all respect, not a well-studied bill. It is a bill that has now come through three times, and in most instances there has been no study whatsoever. When the Senate had the chance to hear on this bill, there was not even a privacy commissioner in place to deal with it, due to the long delay in finding a new commissioner to replace Commissioner Stoddart and later acting commissioner Chantal Bernier.

With respect to the commissioner's support, yes, I too can cherry-pick particular comments from the Privacy Commissioner about where the commissioner supports the legislation, but I can also note that the commissioner's office has been consistent in saying that it finds it problematic with respect to voluntary disclosure, and yet that hasn't changed, and in identifying a number of other improvements.

So the question is this. Is this a well-studied bill that we ought to get on with? With respect, it is both not well studied and ought to be fixed. Canadians deserve better.

The Chair: Go ahead, Mr. Gogolek.

Mr. Vincent Gogolek: I have another quick point, which is that, as I mentioned at the beginning of my prepared remarks, the government has decided to refer the bill to this committee before second reading. Presumably, that is because it is open to amendments beyond the statement of principles of the bill. I find your remarks a little puzzling in terms of the difficulty that could ensue if amendments were to be made. Presumably, the government and the government House leader would have been aware of those difficulties when they in fact took the unusual step of breaking the normal process of things, and referring Bill S-4 to this committee before second reading.

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

We'll move on now to Ms. Nash for eight minutes.

Ms. Peggy Nash (Parkdale—High Park, NDP): Thank you, Mr. Chair.

Thank you to all the witnesses.

I'm puzzled by the line of questioning by the previous member, because clearly it was the government's decision to, first of all, introduce this bill in the Senate and to give it very little review, with very few witnesses, very little oversight, and to take nine years, frankly, to develop this legislation. There's no excuse for that kind of delay.

There was an implicit criticism of these witnesses for not having offered their testimony at the Senate hearings, but there was no opportunity for them to do that. Having said that, their perspective, Mr. Chair, was covered.

The Chair: You have a point of order.

Mr. Mark Warawa: Thank you, Chair.

The comments made by Ms. Nash are not accurate. They've been addressed to me, I believe—

Ms. Peggy Nash: I addressed them through the Chair.

Mr. Mark Warawa: I am speaking to the Chair.

In fact, the question was this. Were the witnesses at the committee as witnesses or did they make submissions? If there was any offence taken, there was no intent to create an offence. It was in fact to ask if they provided testimony or if they provided a submission.

Mr. Chair, we often have submissions presented to you, and those are forwarded on to us, and we find them very valuable and informative. That is a venue for others to provide input and information to this committee so that we can do our work very well. It's important that it be made clear that people can do that.

● (1215)

The Chair: Thanks.

Go ahead. I've stopped the clock, so I'll restart it again.

Ms. Peggy Nash: All right, thank you. That will not be deducted from my time.

The Chair: It hasn't even started yet.

Ms. Peggy Nash: Okay, super, thank you.

I do want to reiterate the point, through you, Mr. Chair, that the point of view that is being expressed by the witnesses here today, and the concerns that they're expressing about Bill S-4 were in fact offered to the Senate committee, but those changes that were recommended were not reflected in the bill that we see before us today. I'm assuming that's what we're being advised of here.

I think the witnesses are raising serious concerns and the Privacy Commissioner, himself, raised concerns about the scope of this bill.

Ms. Lawson, I want to start with you and ask you specifically about the subjective model proposed here for companies determining if there's been a mandatory data breach, disclosure on that. Can you advise us of your interpretation of what could happen with what's being offered in Bill S-4, and how you would recommend tightening up that provision?

Ms. Philippa Lawson: Sure, thanks.

I actually wouldn't call it a subjective test. I think it still is an objective test; the problem is that it's left up to industry to apply that test, and there is not enough oversight or incentive to ensure they are doing it properly.

One solution is to have the Privacy Commissioner be able to review the breaches and determine which breaches require, for example, notification of individuals. This is the model that is being proposed by PIAC, I believe, and it's certainly one that would get around the problem of the industry itself determining whether or not a breach meets the threshold for reporting to the Privacy Commissioner and/or to individuals if you go with a different standard.

I think it is a problem. I guess you can call it a subjective standard, but the problem is that industry is making its own determination, and if you're going to go with that kind of model, then it's all the more important that you have strong incentives in place for industry to comply. Otherwise they won't. It's simply not in their interests, and that's what we're seeing. If you study any aspect of PIPEDA compliance right now, non-compliance is just a cost of doing business right now. That's a fact.

I'm disappointed that the Privacy Commissioner is not really acknowledging that and calling for order-making powers. It's something that's very disappointing to me. As I said already, I had to take the Privacy Commissioner to court in order to get her to exercise her jurisdiction at that time, and it seems that for some reason there is not the appetite that there should be in that office for order-making powers and more effective enforcement of this legislation.

Ms. Peggy Nash: Just so I understand, the test is an objective one, but it is subjective with respect to the private sector if they determine or believe they have breached that level. So, am I to understand that if there were this two-step model in place whereby there was mandatory disclosure to the Privacy Commissioner, then it would be up to the commissioner to determine if the breach should in fact be reported to the individuals affected?

Ms. Philippa Lawson: Yes. To be fair, it is an objective test. If you look, for example, at proposed subsection 10.1(1), it says:

> An organization shall report to the Commissioner....if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.

That is an objective standard. The problem is that we're letting the industry itself make that determination when there is a huge incentive for the industry not to disclose, so either you need much stronger incentives for disclosure or you need a third party, like the Privacy Commissioner, to make that determination, to be able to review it, to have the resources with maybe one or two more bodies in the office to review these much more standard breach notifications and at least determine which ones need to be sent to individuals.

● (1220)

Ms. Peggy Nash: I have one other question for you, Ms. Lawson. You talked about the fines today and the fines contained in Bill S-4as the costs of doing business, and you said they're not a serious enough disincentive to any kind of privacy breach.

What do other jurisdictions have? What would be a serious disincentive that would really encourage the private sector to ensure that it is maximizing privacy protection?

Ms. Philippa Lawson: I think Dr. Geist made a good point in that respect in suggesting that we look at the anti-spam law this government has passed and the attention it's getting from industry. Dollars matter, but it's also the process.

With fines, quasi-criminal fines, that require prosecution and proof of intent, even if they are high, the risk of a company being fined is very low.

What's much more effective are administrative monetary penalties, which can be imposed much more easily without the quasi-criminal process and proof of intent. That's the route we've gone with the anti-spam law and that is the route we should be going with for this law as well.

Another very strong incentive is civil lawsuits. If individuals are able to bring civil lawsuits or class action suits against companies, that can be a very strong incentive. It's not a strong incentive under this regime because it's too difficult to do so, because there are no damages for embarrassment in it. That's been taken out. It has to be humiliation, so it's a high standard, and there are not a lot of dollars an individual would get even if they were able to sue.

There are different ways. The third type of incentive is bad publicity, but once again we're not seeing that being used very often by the Privacy Commissioner. This regime—when you look at section 20, which does allow for disclosure by the Privacy Commissioner if it's in the public interest—starts out by saying that there shall be no disclosure of this breach through reporting.

Why not? Why not make that a transparency reporting thing? Why not use bad publicity?

So there are three types of financial incentives that can be used, and I don't feel that any of them are being used to the optimum under this proposed legislation.

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

Now on to Madam Gallant, for eight minutes.

Mrs. Cheryl Gallant (Renfrew—Nipissing—Pembroke, CPC): Thank you, Mr. Chair.

First of all, I have a question for Professor Geist. You mentioned that you had concerns about warrantless disclosure of information on the part of telecoms.

Where in this legislation would you be applying warrants?

Dr. Michael Geist: What I said was that I'm concerned about disclosure without a warrant and without consent, or without knowledge.

Warrants involve situations where we have disclosures to law enforcement. Where this law applies is not to law enforcement, but rather to voluntary disclosures to non-law enforcement.

We've seen under PIPEDA, the existing system, the ability for organizations, where they are conducting investigations or potential lawsuits, to go to get the necessary court orders for disclosure of that information.

In a number of those kinds of cases what the courts do is to set real conditions around that disclosure. There is both oversight as to when those disclosures occur, and then clear limitations on how that information may be used, including to whom it may be further disclosed, and the need to destroy it—a whole series of conditions recognizing the privacy import of that information.

What this bill does is to expand voluntary disclosure of that information without court oversight and without any limitations.

● (1225)

Mrs. Cheryl Gallant: This bill does not pertain to law enforcement. What you're referring to are bills that would pertain to law enforcement.

Dr. Michael Geist: No. What I'm referring to is an organization that has my information. There may be instances where they are disclosing it either to law enforcement or to private sector organizations.

In the law enforcement context, if it's a warrant, and post the Spencer decision, it's quite clearly now going to be a warrant, or should be a warrant.

In the private sector what this bill does is to say that we can disclose information on a voluntary basis without a court order and without any sort of court oversight.

I'm saying that, over the last number of years under PIPEDA, we've had cases where organizations have said that they want to identify who those subscribers are because they want to sue them, and there's an instance where they are conducting this investigation or have this legal process. The court examines the circumstances around whether there's an appropriate case to order that disclosure and sets limitations on the disclosures that can occur.

What Bill S-4 does is to expand the prospect of that kind of disclosure on a voluntary basis.

Mrs. Cheryl Gallant: So the disclosure that's required by this bill is on the part of companies when there's a data breach.

Dr. Michael Geist: No, not a data breach at all. The language used in Bill S-4 is exceptionally broad. It refers to the ability to disclose this information—here, I can try to call it up for you—where it is reasonable for the purposes of investigating a breach of an agreement or a contravention of a law that's either been, has been, or might even be committed, and where it is reasonable to think that if the individual were made aware of that disclosure, it would compromise the investigation.

We're not talking about data breaches here; we're talking about virtually carte blanche voluntary disclosures.

Mrs. Cheryl Gallant: That part of the bill refers, as I read it, to the internal investigations of an organization where they're looking for internal fraud.

Dr. Michael Geist: There's no reference to internal organizations nor internal fraud. The new (d.1) is talking about “a breach of an agreement or a contravention of the laws of Canada or a province” that's either been committed or, even, that might be about to be committed. It's anticipatory: I think something might happen, and so I'm going to move forward. We're talking about breach of contract even. Someone could then say that I'm entitled to voluntarily disclose. The notion that Canadians ought to be assured that there's a reasonableness standard in there doesn't strike me as providing much comfort whatsoever. This is very broad. There are no limits and there are no clear limits, limits other than that reasonableness, but that's a very limited standard, and there are no limitations set on what can happen to that information afterwards. We're not talking about security breach. We're not talking about fraud. We're not talking about internal investigations here. We're talking about something much, much broader.

Mrs. Cheryl Gallant: Okay, thank you, for now.

Ms. Lawson, you said that the terms of service are too long and people don't bother to read them. The onus is really on the person who clicks on the “Accept”. If this is too long and onerous for the person to read through, and we're letting them be bereft of responsibility for what they're accepting, what is it that you want to see on that page where people read through and click to accept?

Ms. Philippa Lawson: If you're going to rely on consent and you want it to be meaningful, then forget negative-option or hidden consent. Everyone knows that no one has the time to read or the ability to figure out where it is hidden in the 20 pages of fine-print legalese. Let's go with real, meaningful consent, which is affirmative opt-in express consent, for all non-essential collection, use, and disclosure of personal data.

What that would mean is that you would have to click “I agree” to the specific disclosures. They would be optional. PIPEDA, as it stands, requires that non-essential collection, use, and disclosure of personal data be optional. The problem is that it allows negative options, hidden options. The hiding needs to be changed. They need to be brought out in the open and it needs to be opt-in consent. Customers must not be forced to consent to things that are not necessary, like marketing.

● (1230)

Mrs. Cheryl Gallant: Okay, so it's not the length of the text or the legalese, it's the hidden negative options. Thank you.

Now you had said that you do support the protective measures in this legislation. The measures that are put forth to protect consumers, how do you see them as being beneficial? What is it that they're doing, in your mind?

Ms. Philippa Lawson: Sorry, I'm not sure what you're referring to. Is it something in Bill S-4?

Mrs. Cheryl Gallant: You said there are positive aspects of the measures in Bill S-4.

Ms. Philippa Lawson: Well, certainly giving the Privacy Commissioner the power to make and enforce compliance agreements is a step forward. It's not nearly as great a step as should be in here, but it's something. Certainly having the security breach notification regime, some kind of regime in place, for reporting to the commissioner and to individuals is better than nothing, in my view. However, this is not nearly as good as it could be. We've been calling for this for 10 years, looking at it and studying it. At this point in time, there's so much experience in other jurisdictions, we should be getting it right. There's no excuse for not doing a better job.

Mrs. Cheryl Gallant: Okay.

Mr. Gogolek, you said that there's no surefire way of saying that provincial policy doesn't cause harm. You said that the way the policies were written in B.C. and Alberta, there was still the potential for harm to be done to the people they're supposed to be protecting.

Can you give any evidence or examples of where there is a potential for a breach under the provincial legislation this is supposed to be mirroring?

Mr. Vincent Gogolek: Are you referring to the quote from the commissioner's report on PIPA? In that report the commissioner said that because we don't have the reports in terms of the information being made available, she is unable to tell. This was in relation to Professor Geist's report. This indicates the difficulty our commissioner in British Columbia has because she is not being made aware of what's going on. It highlights the importance of the commissioner being made aware of these situations as much as possible, partly for systemic reasons, but also to know what's going on.

The Chair: Thank you, Madam Gallant.

We'll now go to Madame Papillon for eight minutes.

[*Translation*]

Ms. Annick Papillon (Québec, NDP): Thank you very much, Mr. Chair.

Mr. Geist, thank you for being here today.

During a Senate committee meeting, you gave the example of California, which requires the disclosure of any security breach related to unencrypted personal information when there are reasonable grounds to believe that the information was acquired by an unauthorized person.

Could you give us a concrete example to explain the impact that a similar definition might have on the application of Bill S-4?

[*English*]

Dr. Michael Geist: Thanks for raising that. It's worth noting that this whole notion of security breach disclosure actually originated out of California, with the idea of creating sort of the perfect world of incentives for companies to do a better job of securing the information, because they don't want to have to go through the cost and potential embarrassment of disclosure. At the same time, it creates incentives or protection for users because they become aware of these disclosures when they happen.

What we've got under Bill S-4 is such a high threshold, and I think Ms. Lawson referenced this as well, that if the standard is only a real risk of significant harm and we don't have big penalties associated with non-disclosure to begin with, at least if you're a larger organization, in many instances, I think it's going to be quite rational, frankly, for an organization not to disclose. They're going to ask, first, what's the risk that anyone will ever find out about this? Second, if they do happen to find out about it and someone shows that there was a real risk of significant harm, then we will face a penalty. But even there, the penalties are relative low.

So what the California law does is to say that we want to ensure that if we're going to err on one side or the other, it's will be to err on the side of trying to mitigate against identify theft, to err on the side of ensuring that there is better security, and by lowering the threshold. We tried to do that a little bit in Bill C-12 and Bill C-29 with the two-step process, so that at least you are made sure that the Privacy Commissioner would be aware of the circumstances where there's a material breach. But in doing away with all of that, I don't think it's just a fear that breaches will occur in Canada. I think these should be expected. And if you asked many Canadians, they would tell you, “Boy, I should have been told about that”. And yet they won't be because companies are going to err rationally, based on the way this law is drafted, on the side of not disclosing it.

● (1235)

[*Translation*]

Ms. Annick Papillon: Thank you.

I will continue with you, Mr. Geist.

During the Senate committee meeting, you also said that creating compliance orders would be founded if accompanied by the powers required to impose sentences or take regulatory actions, as is the case in the United States, where compliance orders are customary.

Could you explain in more detail what necessary powers we lack in Canada?

[*English*]

Dr. Michael Geist: What we lack is both tough penalties, as we've talked about, and order-making power for the commissioner to order someone to comply with rules, as is found even at the provincial level. The prospect of negotiating compliance agreements is certainly better than what we have now. I don't think anybody disputes that. Nonetheless, it's essential that we do better and provide the commissioner with real powers to be in a position to ensure that organizations are more likely to comply. I think it's striking that people often reference the United States and will argue that in the U. S. they have no broad-based privacy law as we do in Canada, and for a long time Canadians have said that we are much further ahead than the U.S., that we at least have this broad-based privacy law. However, the reality is that the Federal Trade Commission, through its order-making power and its power to truly enforce, has been able to exact far tougher penalties and far stronger levels of compliance than the comparable here in Canada because our commissioner simply hasn't been granted those kinds of powers.

[*Translation*]

Ms. Annick Papillon: What you are saying is interesting.

Let's come back to Quebec. Quebec legislation relating to the protection of digital privacy sets out exceptions that allow a business to gather or disclose any personal information without the consent of the individual concerned, but these exceptions are very limited and include, for example, situations involving a criminal investigation.

Do you think Bill S-4 could be inspired by what has been done in Quebec?

[*English*]

Dr. Michael Geist: I don't have expertise in the Quebec law per se, but there is a series of exceptions, quite clearly, even as it stands now under PIPEDA. So when we talk about substantial similarity between the provinces that have these kinds of laws, I think what you're saying is somewhat consistent with that.

I really think what this would do, though, especially on that voluntary disclosure, is move us far beyond where I think most Canadians would expect in terms of the potential disclosure of their information without setting the sorts of oversight and kinds of conditions that would otherwise be appropriate.

[*Translation*]

Ms. Annick Papillon: So Bill S-4 would give the privacy commissioner new powers to conclude compliance agreements with organizations. Are you afraid that the commissioner would be overwhelmed if every breach is reported to him?

I think you suggested that at the start of your speech.

[*English*]

Dr. Michael Geist: I think that if every time a USB key went missing, there were requirements to disclose, then yes, you would find that organizations would be spending a lot of time disclosing. However, if we look back at the Bill C-12 and Bill C-29 standard, that's not the standard we talked about. It set a material breach as the standard.

You can debate whether or not that's the appropriate standard, but at a minimum it gets us at a number of breaches that this law will not. Moreover, it does so in a way that I think was good for companies too, because rather than companies being faced with this either/or of going to the expense and potential embarrassment of simply disclosing or not, it said as an intermediary step, let's discuss this on a confidential basis with the Privacy Commissioner's office and determine whether or not it warrants that broader disclosure.

Frankly, that was a good thing for organizations to potentially avoid having to make those broader disclosures, in some circumstances, and it provided the comfort of ensuring that users knew that, at a minimum, we had an advocate, the Privacy Commissioner, who was going to be made aware of these circumstances.

It's puzzling to me why this was removed in favour of a process that, frankly, does less to protect Canadians and, ultimately, actually can create larger costs for companies as well.

● (1240)

[*Translation*]

Ms. Annick Papillon: Thank you, Mr. Geist.

Ms. Lawson, I think you wanted to address—

[*English*]

Ms. Philippa Lawson: If I could just quickly jump in, if there's no requirement to report a certain class of security breaches, there's no incentive for the company to avoid them.

[*Translation*]

Ms. Annick Papillon: Okay.

Mr. Vincent Gogolek: I would like to talk about another aspect relating to what Professor Geist mentioned.

This also imposes a kind of penalty on companies that are more considerate about protecting our privacy. In fact, the companies that are the most open and that will inform more people if they encounter a privacy-related problem will see their reputation pay the price.

Those companies that take a chance and try to hide things or who see the situation and decide to do nothing, it is always possible that no one will know that there was a problem or a breach. That isn't the situation we should create. We need to have minimum standards so that everyone knows what their level of behaviour should be.

[*English*]

The Chair: Thank you very much.

[*Translation*]

Thank you very much, Ms. Papillon.

[*English*]

I just want to let the witnesses know that our final questioner is coming up and I'm looking at the time. Our clocks are about three minutes slow, by the way, going by our BlackBerry time, but I wanted you to be aware that we'll probably have the ability to give each of you two minutes to wrap up. So if there are some final points you want to make, then keep that in mind as Mr. Lake begins his questioning.

Mr. Lake, you have eight minutes.

Hon. Mike Lake (Edmonton—Mill Woods—Beaumont, CPC): Thank you, Mr. Chair.

I found it interesting to listen to all of the testimony first before getting a chance to talk.

Ms. Lawson and Mr. Geist both made similar statements. I wrote down that Ms. Lawson said, “We should be getting it right” and Mr. Geist that “We have to get it right”.

Interestingly, of course, I think that when we have these hearings, “right” means “the way you want it”. Ultimately, there have been other witnesses who have come before committee and said very different things. If the definition of “getting it right” means, for example, agreeing with those who said that consent provisions go too far, which we heard in the previous meeting, I don't imagine you would think it means we're getting it right.

Someone said that our data breach reporting regime is too onerous. If we decided that was the direction to go in, I'm quite certain that neither of you would say that this is “getting it right”. When anyone uses this term, I always hearken back to our hearings on anti-spam and copyright and even UBB. People's definitions of getting it right are very different. As in those cases, we're left to try to find the balance between very different, competing positions, and I think the case with this bill is no different.

Taking a look at three of the areas that have come up, I find it interesting....

Ms. Lawson, I'm going to come to you first and deal with section 20. You mentioned you had some concern with that section, I think around the confidentiality provision written into Bill S-4.

Ms. Philippa Lawson: Yes.

Hon. Mike Lake: Do you have the bill in front of you?

Ms. Philippa Lawson: Yes, I do.

Hon. Mike Lake: Can you read that to me?

Ms. Philippa Lawson: Do you mean proposed subsection 20 (1.1)?

Hon. Mike Lake: Yes.

Ms. Philippa Lawson: It reads:

> Subject to subsections (2) to (6), 12(3), 12.2(3), 13(3), 19(1), 23(3) and 23.1(1) and section 25, the Commissioner or any person acting on behalf or under the direction of the Commissioner shall not disclose any information contained in a report made under subsection 10.1(1) or in a record obtained under subsection 10.3(2).

Hon. Mike Lake: Perfect. Do you have PIPEDA in front of you as well?

Ms. Philippa Lawson: I'm sorry...?

Hon. Mike Lake: Do you have PIPEDA, the actual legislation, in front of you as well?

Ms. Philippa Lawson: Yes, I do.

Hon. Mike Lake: Can you read subsection 20(1), the one that is already in the act, and tell me how the two differ?

Ms. Philippa Lawson: The only difference is that proposed subsection 20(1.1) just adds the breach notification.

Hon. Mike Lake: So the new provision in Bill S-4 really just makes the new legislation consistent with the old. Is that correct?

● (1245)

Ms. Philippa Lawson: Well, it decides to treat breach.... Yes. I mean, effectively yes; it treats breach notification in the same category as everything else.

Hon. Mike Lake: In this area, then, the real impact, as far as our talking about the powers of the commissioner is concerned, happens in proposed subsection 20(2), I believe, where it states:

> The Commissioner may, if the Commissioner considers that it is in the public interest to do so, make public any information that comes to his or her knowledge in the performance or exercise of any of his or her duties or powers under this Part.

In other words, it is in giving the commissioner the power to name and shame organizations that don't follow the law.

Ms. Philippa Lawson: Yes.

Hon. Mike Lake: That is a very significant power, if you think about organizations that may have been publicly identified as breaching privacy law. We can point to several examples in which I would say it would be—

Ms. Philippa Lawson: That's right. In the present writing, the subsection overrides the confidentiality.

Hon. Mike Lake: So I would certainly say that this new provision, in this bill, has some teeth.

I want to go to proposed section 6 with you as well, if I may, because I found your comment about its being an elephant in the room interesting. You talked about the pretence that companies are obtaining consent.

As I read it, as I look at the new legislation as written and as you identified, it uses the phrase “an individual”. It says here that it is

> valid if it is reasonable to expect that

—and this is the part that you had an issue with, but that I actually love—

> an individual to whom the organization’s activities are directed

—so basically any individual—

> would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.

So it is for everybody. It doesn't just single out kids or any other particular group of the vulnerable; it actually applies to everybody. That consent is only valid if it is reasonable to expect that an individual to whom you're targeting your activities would understand the nature, purpose, and consequences of the collection.

You talked about the elephant in the room. I agree with you. I often think that clicking a mouse to try to get through to something else that you want to use on the Internet is just too easy. I think this clarifies that people need to understand the nature, purpose, and consequences. Don't you agree?

Ms. Philippa Lawson: I agree, and I like the section for that reason. It provides the clarification that the industry needs. However, the point I'm making is that those additional words that are not in the formulation from Bill C-12 actually restrict the application of this. They do not expand it; they restrict it. The earlier formulation was that consent is only valid if it's reasonable to expect that the individual understands it. That means that it has to be reasonable to expect that the individual in question in that particular transaction understands it. So the earlier formulation covers everyone. If it's a child, if it's a senior, whoever it is, that individual needs to be able to understand it.

The new formulation restricts it. The new formulation says that you only have to worry about individuals to whom you are directing your activities, and it's very easy for an organization to say, "We are directing our activities to adults, not to children."

Hon. Mike Lake: If some 11-year-old decided that he or she wanted to sign up for a service at an organization that's clearly directing its activities towards adults—for whatever reason there are no parental controls on the computer or there's not proper supervision for the kid—I think it's ridiculous to assume that organization would somehow be able to know that. I don't know how you would possibly do that.

Ms. Philippa Lawson: If you're looking at the protection of children, in the United States there's specific legislation called the Children's Online Privacy Protection Act. It may be a good place to start if what you want to achieve is the protection of children.

I don't think that proposed section 6.1 achieves protection of children. I think it—

Hon. Mike Lake: It's an interesting dynamic, though, because I think—

Ms. Philippa Lawson: It does help clarify generally what you need for consent.

Hon. Mike Lake: I think what you're raising is probably a really important issue as well, something that probably falls outside the scope of this piece of legislation, but probably inside the scope of a lot of the legislation that we're moving these days. That might be a conversation for another day.

When we look at clause 7 and the private investigations, I found Ms. Borg's comments interesting. She seemed to suggest that somehow we should peer into the future, to see what provincial legislatures might actually do with their legislation—and she used the word "proactively" to make that change now. I don't know how we can do that. I'm not sure how we would presume to know what legislators at the provincial level will do. What we do know is what they've done, which is to pass legislation in this area that is very similar to what we're doing now to try to be consistent with what they're working on.

● (1250)

Ms. Philippa Lawson: I have a point on that, and again it's something that I'm not understanding. In this regime, the federal government is supposed to be leading and the provinces are supposed to be passing substantially similar legislation. If the provincial legislation is substandard and not achieving the level of protection that Canadians deserve, then—

Hon. Mike Lake: But, to be fair, no one is actually saying that the provincial legislation is substandard and no one's able to point to anything that's wrong with the provincial legislation. Two provinces have almost identical wording in their legislation.

Ms. Philippa Lawson: Well, I pointed out something in Alberta's legislation that people seem to be ignoring, but I think you've heard from Dr. Geist about problems at the provincial level. We're simply not hearing about it because there's no transparency.

Hon. Mike Lake: Dr. Geist is a smart guy, but sometimes we disagree.

The Chair: On that note, I'll go in reverse order, for fairness.

Ms. Lawson, I'll give you two minutes for some closing remarks.

Ms. Philippa Lawson: Chair, thank you very much.

I guess it's just a minor point, because I think I didn't make it in my submission. I agree entirely with the comments of my colleagues about the need for a dual standard for breach notification, with more breach notification to the Privacy Commissioner and commissioner playing a greater role in determining which breaches need to be disclosed to individuals.

I would just go back to my earlier point. I think there are three fundamental areas of Canadian privacy that this legislation needs to protect. There need to be more hard limits on what companies can do with our personal information, particularly for children and vulnerable people. Second, consent needs to be real. That means express, opt-in consent, not negative option. Third, there need to be order-making powers and administrative monetary penalties for non-compliance.

Thank you.

The Chair: Thank you, Ms. Lawson.

We'll now go to Dr. Geist.

Dr. Michael Geist: I'll close by responding to what Mr. Lake noted regarding what happens when witnesses talk about getting it right. I will just provide two things, first to note that the government has painted this legislation as being pro-consumer—obviously part of the digital economy strategy—which makes it clear what the intent of the legislation is. I think it is difficult to say that you're getting that balance right, particularly when the legislation is framed as trying to protect consumers and being pro-consumer, when you have those same pro-consumer groups and even the Privacy Commissioner pointing to problems, such as the voluntary disclosure provision. To me that means that balance isn't getting struck appropriately.

Even more, my reference to getting it right really wasn't in terms of the substance, but rather to say that we should not be cautious about amending the legislation where there is a belief that it can be improved. The question was raised—and my apologies if I got more passionate than I might usually get on this issue, but this is an issue that we have spent many years focusing on—that if we are all in agreement that privacy is important, surely we can give this bill, including potential amendments, the same kind of priority we're providing Bill C-51 with, which is also clearly on a bit of a rocket docket, with perhaps not even the Privacy Commissioner getting to testify on it.

There is an opportunity to do so, if we're going to think about how privacy and security often go hand in hand. If we're prioritizing Bill C-51, we can similarly prioritize Bill S-4 and find a way to get this bill, with some amendments as necessary, done and passed through the Senate and back into the House so that when an election comes, Canadians can look at a piece of legislation and say that it really does reflect the kinds of concerns they have with respect to privacy.

The Chair: Thank you very much.

Mr. Gogolek for a two-minute closing, please.

Mr. Vincent Gogolek: Thank you for having us here. This is a very important piece of legislation. It's also very important that we look at it in the context of things that have been happening, as it winds its way through the legislative process. Since the Senate hearings, we have had the Spencer decision by the Supreme Court of Canada. We have also had the report from the special legislative committee looking at PIPA in B.C. These are new developments. They are bringing information to you that you probably will want to look at.

We're also encouraged by the fact that the government has seen fit to bring this legislation to this committee before second reading. I think that shows that the government is in fact open to a wider array of amendments than before, than there would normally be in the course of the legislative process, which is important for the committee to keep in mind.

Furthermore, there will be a federal election later this year and, as you're looking at how companies deal with our personal information, Canadians will be asking questions about how their political parties are dealing with the personal information they store, collect, use, and disclose. It is important that you do that. Bringing the parties under PIPEDA, in whatever form the legislation is ultimately amended, would be a major improvement. I urge you to do that.

Thank you.

● (1255)

The Chair: Thank you very much.

Thank you to all of our witnesses. We appreciate your time and your expertise.

Colleagues, we are adjourned.