HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Industry, Science and Technology

INDU • NUMBER 034 • 2nd SESSION • 41st PARLIAMENT

EVIDENCE

Tuesday, February 17, 2015

Chair

Mr. David Sweet

Standing Committee on Industry, Science and Technology

Tuesday, February 17, 2015

● (1100)

[*English*]

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

Welcome to the 34th meeting of the Standing Committee on Industry, Science and Technology where pursuant to the order of reference of Monday, October 20, 2014, Bill S-4, an act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another act, is what our study is right now.

We are grateful to have before us the Privacy Commissioner of Canada, Daniel Therrien. With him are Patricia Kosseim and Carman Baggaley.

We have a second panel at noon, colleagues, so we will begin with the Privacy Commissioner's testimony and then our rounds of questions.

Mr. Commissioner.

[*Translation*]

Mr. Daniel Therrien (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): Thank you, Mr. Chair. Good morning, members of the committee.

Thank you for the invitation to present our views on Bill S-4, An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act.

With me today are Patricia Kosseim, senior general counsel, and Carman Baggaley, senior policy analyst.

Ms. Kosseim and Mr. Baggaley appeared before the Standing Senate Committee on Transport and Communications on Bill S-4, shortly before my appointment as Privacy Commissioner was confirmed. My views on Bill S-4 are largely in line with the office's position as presented at that time.

I will however be addressing in more detail the proposed amendment that allows organizations to disclose personal information to other organizations without consent. I will also discuss paragraph 7(3)(*c.1*) disclosures in light of the Supreme Court's Spencer decision.

Let me first say that I am greatly encouraged by the government's show of commitment to update the Personal Information Protection and Electronic Documents Act, and I generally welcome the amendments proposed in this bill.

Proposals such as breach notification, voluntary compliance agreements and enhanced consent would go a long way to strengthening the framework that protects the privacy of Canadians in their dealings with private sector companies.

Mandatory breach notification will bring enhanced transparency and accountability to the way private sector organizations manage personal information. I support the risk-based approach that will require organizations to assess the seriousness of each incident and its impact on affected individuals.

I believe that the organization experiencing the breach is in the best position to assess risk and decide whether notification of individuals is warranted. Requiring organizations to keep a record of breaches and provide a copy to my office upon request will give my office an important oversight function with respect to how organizations are complying with the requirement to notify.

The proposed voluntary compliance agreements will enhance my office's ability to ensure, in a timely and cost-effective manner, that organizations are meeting their commitments to improve their privacy practices without having to resort to costly litigation before the Federal Court in conditionally resolved cases.

● (1105)

[*English*]

As for the proposed provision that aims to enhance the concept of valid consent, I believe that this is a useful clarification of what constitutes meaningful consent under PIPEDA. It underscores the need for organizations to clearly specify what personal information they're collecting and why in a manner that is suited to the target audience.

While I support many of the amendments proposed in this bill, I nevertheless have strong reservations about proposed paragraphs 7 (3)(d.1) and (d.2). These proposed provisions would allow an organization to disclose personal information without consent to another organization in certain circumstances. My concerns are twofold.

First, I believe that the investigative body regime as it currently exists in PIPEDA and which paragraph 7(3)(d.1) and (d.2) seek to replace provides important transparency and accountability safeguards that will disappear with the proposed amendments.

Currently under PIPEDA, organizations can disclose personal information without consent to investigative bodies designated through a transparent governor in council process. The list of organizations with investigative body status is publicly available. Under the proposed amendments, potentially any organization will be able to collect or disclose personal information for a broad range of purposes without any mechanism to identify which organizations are collecting or disclosing the information and why.

Furthermore, the proposed provisions seek to dilute the thresholds and grounds for disclosure that currently exist under the current investigative body regime in paragraph 7(3)(d). I would prefer to maintain the existing investigative body regime. However, if that is not possible, then I would recommend keeping the existing PIPEDA thresholds found in paragraph 7(3)(d) and grounding disclosures in real problems rather than fishing expeditions.

This would mean three things: first, the threshold under paragraph 7(3)(d.1) should be based on a "reasonable grounds to believe" that the information relates to an actual breach or contravention; second, the threshold under paragraph 7(3)(d.2) should be based on a "reasonable grounds to believe" that the information relates to the detection or suppression of fraud that "has been, is being or is about to be committed"; and third, disclosures under paragraphs 7(3)(d.1) and 7(3)(d.2) should only be permitted on the initiative of the disclosing organization.

In addition a mechanism for enhancing transparency and accountability around these disclosures would be needed. For example, disclosing organizations could be required to issue transparency reports and to document the analyses undertaken in deciding to disclose under these provisions.

[*Translation*]

Finally, I would like to address the Spencer decision and how I believe it impacts paragraph 7(3)(*c.1*) of PIPEDA.

ln the Spencer decision, the Supreme Court held that police need a warrant or a court order when seeking subscriber information from an organization subject to the act.

ln the court's view, there is a reasonable expectation of privacy in subscriber information connected with online activity and the police request that the organization voluntarily disclose this information constituted a search that violated the Charter. I believe that this decision is a significant step forward in protecting privacy, but it leaves unanswered the question of what types of information attract a reasonable expectation of privacy and the related question of when organizations may voluntarily disclose other types of information in response to a police request.

As a result, organizations are left in a state of uncertainty and ambiguity as to when they may or may not disclose personal information without warrant and it leaves individuals in the dark about when their personal information may be disclosed to state authorities without their consent or prior judicial authorization.

I would therefore urge the committee to recommend putting an end to this state of ambiguity by clarifying when, post-Spencer, the common law policing powers to obtain information without a warrant may still be used. I believe that a legal framework, based on the Spencer decision, is needed to provide clarity and guidance to help organizations comply with PIPEDA and ensure that state authorities respect the Supreme Court of Canada's decision.

More specifically, I would recommend that Parliament provide greater clarity and transparency by amending PIPEDA to define "lawful authority" for the purposes of paragraph 7(3)(*c.1*) in line with the Supreme Court's decision, that is, where there are exigent circumstances, pursuant to a reasonable law other than paragraph 7 (3)(*c.1*), or in prescribed circumstances where personal information would not attract a reasonable expectation of privacy.

Thank you for your attention. I would be happy to answer any questions you may have.

● (1110)

[*English*]

The Chair: Thank you very much, Commissioner, for your testimony.

Colleagues, based on the time we have, we'll do our ususal when we have two panels, which is five minutes each.

We'll begin with Mr. Lake.

Hon. Mike Lake (Edmonton—Mill Woods—Beaumont, CPC): Thank you to the witnesses for coming today.

Mr. Therrien, when was the last time PIPEDA was changed?

Mr. Daniel Therrien: Certainly several years ago. I understand this bill is the outcome of a five-year review of PIPEDA called for in the original legislation.

Certainly I support the bill, subject to two amendments, but generally I support this bill.

Some of the provisions in this bill are overdue in my opinion, particularly the requirement for mandatory notification in the case of breaches.

As to the date....

Ms. Patricia Kosseim (Senior General Counsel and Director General, Legal Services, Policy and Research, Office of the Privacy Commissioner of Canada): The last round of amendments to PIPEDA would have come into force with the CASL legislation that made consequential amendments to PIPEDA in light of the anti-spam legislation. I believe that may have been the last time, but certainly there was no full review as per the requirement of the act.

Hon. Mike Lake: It has been several years since we went this deep into PIPEDA as a Parliament.

In terms of the work that your office does, how will the legislation as proposed right now change the operations of your office?

Mr. Daniel Therrien: I think there are two main amendments that are very necessary and that will be helpful for us to implement and apply.

I refer to the obligation imposed on organizations to notify the OPC and the concerned individuals in the case of data breaches. We know from media reports and other information that data breaches are an important and growing phenomenon both for public and private institutions, and we think it will be an important progress in PIPEDA to have this regime of mandatory breach notification.

We think, obviously, that there will be repercussions on resources. We currently have a voluntary notification process applicable to private organizations in the case of breaches. From year to year we see there are fluctuating numbers, but there are approximately 60 notifications under that regime. We expect that the number will increase significantly with mandatory breach notification. That was the experience in Alberta when the voluntary scheme became mandatory. There will be an impact for sure. Overall, we think that this is a very positive development.

In addition to that, a second major amendment that I would mention has to do with compliance agreements. We seek to work with organizations to promote compliance with PIPEDA. This means in some circumstances that following complaints, we engage in discussions with organizations on resolving complaints conditionally, meaning that organizations change their practices in order to be more compliant with PIPEDA. The mechanism of compliance agreements would further enhance that capacity.

Hon. Mike Lake: I have one minute to talk about valid consent. I know that it doesn't apply specifically just to kids, but a lot parents would be interested in some of the changes being made in that area.

Could you give an example of the type of thing that we're dealing with when we talk about enhancing the concept of valid consent?

● (1115)

Mr. Daniel Therrien: Currently, PIPEDA is based in large part on the concept that information is to be collected and used with the consent of the individual to whom it pertains, and that deals with a private organization. That concept is not defined; nevertheless, it has been the subject of many investigations and pronouncements by the office.

We think that the proposed definition of consent would be useful. It may not be absolutely necessary; we already have a concept that is workable, but I think it would be useful to further clarify that consent is to be evaluated from the perspective of the person whose consent is invoked. Organizations would be asked to put themselves in the shoes of the various clientele from whom they are collecting information so that consent is as meaningful as possible.

That would be useful.

The Chair: Okay, thank you, Mr. Commissioner.

Now we go to Ms. Nash for five minutes.

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

[*Translation*]

My thanks to you, Mr. Therrien, and to your team for joining us today to give testimony before our committee.

[*English*]

I have two questions that I hope I have time for.

The first concerns the point that you made to ensure that this legislation is compliant with the R. v. Spencer decision, and like you, we support the need for this legislation and believe that it is long overdue.

In your testimony, you argued for better clarity for organizations around disclosure and also clarification for individuals. The British Columbia Legislative Assembly has just published a report on their review of their Personal Information Protection Act, PIPA, in which they suggest amending articles in the bill that allow for voluntary warrantless disclosure, very similar to the articles in PIPEDA, and they are doing this as a response to this court decision, fearing a charter challenge.

Do you think that adds weight to your recommendation that the government should avoid any potential court challenge and amend this legislation to reflect the concerns that you raised here before the committee?

Mr. Daniel Therrien: Thank you for the question.

Frankly, I haven't read the amendment proposed in the B.C. legislation, so I can't comment on that particular formulation, but I'll say a few things.

Point one, the Spencer decision is a huge development for privacy law. It is very helpful; it has set already very good parameters for the collection of information without warrants, by prescribing that police agencies—the state—need a warrant to collect information when that information relates to the activities and interests of individuals on the Internet. That is already a very good starting point.

There is an issue, though, that has not been clarified by the Supreme Court, nor could it be, I think. It left the possibility of the collection of information without warrant when there is no reasonable expectation of privacy.

Following Spencer, we have heard from various private organizations how they intend to apply this, and we have seen variances. We've also seen various interpretations of it by government departments.

That brings me to the view that we're starting from a very good starting point with the Supreme Court's decision, but given the ambiguity and the different interpretations given by private organizations and government departments, I think it would be useful if Parliament were to provide clarity, in having a regime that would set out, explain, define in what circumstances there is no reasonable expectation of privacy. With this, ultimately Canadians would have a much better sense of what type of information and in what circumstances the information they put on the Internet might be collected without warrants by state authorities.

● (1120)

Ms. Peggy Nash: Thank you. That's helpful. The minister said that he thought the existing bill was already compliant with R. v. Spencer, so that information is helpful.

I also want to ask you, because you argued for the existing investigative body regime under paragraph 7(3)(d), but described another potential approach, to tell me why the current regime of oversight is preferable, in your view.

Mr. Daniel Therrien: It's for two reasons, essentially.

Point one, I totally agree that there needs to be provision in PIPEDA allowing organizations to address the issue of fraud or breaches of agreements that they may face. The question is how to do it. The current regime, I think, is preferable to what is proposed in Bill S-4 in that, first, it does not allow for fishing expeditions, so that the threshold for the suspicion an organization has that there might be fraud involved is at a higher level, which I think is preferable. Second, the investigative body regime calls for transparency and publicity—we know what the investigative bodies are—as opposed to the proposed modifications whereby any organization could share information with any other organization, so that there would be less transparency, as well as room ultimately for fishing expeditions.

The Chair: That's all the time we have there.

We'll go to Mr. Carmichael for five minutes.

Mr. John Carmichael (Don Valley West, CPC): Good morning to you and your colleagues, Commissioner.

Commissioner, in your opening comment or, I believe, in an answer to my colleague's question, you mentioned that data breaches are a common and growing phenomenon and that annually you receive some 60 notifications.

Is that correct? Is that approximately the right number?

Mr. Daniel Therrien: Yes. The number fluctuates, but it's roughly 60.

Mr. John Carmichael: With mandatory notification, this will increase as we go forward

Mr. Daniel Therrien: Yes.

Mr. John Carmichael: Could you tell us how the requirement to maintain records of data breaches will increase your office's ability to provide oversight and enforce the obligation to notify individuals of data breaches that present a real risk of significant harm?

Mr. Daniel Therrien: The requirement in question would require organizations to keep records of data breaches of any kind. We will be able to review their records to determine whether or not appropriate breach notification has occurred, and it will allow us to determine trends generally on the issues so that better advice can be given to organizations and individuals.

In part this provision that you're referring to will allow us to determine whether the organizations are complying with mandatory breach notifications. If they are not, in the worst-case scenarios, we could advise police authorities and the Attorney General so that prosecutions could be made against these organizations. So it's a clear incentive for organizations to comply with the requirement.

Mr. John Carmichael: Would these records be maintained by your office, or is it the requirement of the corporations to retain those records?

Mr. Daniel Therrien: The corporations would have the obligation, and we would have the ability to review these records.

Mr. John Carmichael: Thank you.

I wonder if you could explain in a bit further detail, then, the new enforcement tools that will give the bill and give you and your office greater authority.

Mr. Daniel Therrien: I believe you are probably referring to compliance agreements—

Mr. John Carmichael: Sorry, yes.

Mr. Daniel Therrien: —so I'll ask my colleague Madam Kosseim to answer your question.

Ms. Patricia Kosseim: Thank you for the question.

Currently under PIPEDA there is a requirement to complete the investigation within a prescribed time period, and there are 45 days after which either the complainant or the commissioner can proceed to court for a *de novo* hearing in the event that we cannot resolve a matter with an organization.

As we've experienced in practice, 45 days is a very short time period to resolve some of the highly complex technological issues or broader accountability issues that organizations quite rightly need time to rectify, so we have developed a mechanism to allow organizations the time to put in place our recommendations. We then follow up with them several months, if not a year, afterwards to ensure they did follow through on the recommendations they said they would undertake to do.

The problem is that in those circumstances, our ability to go to court can be challenged if we're outside the prescribed period. I think the compliance agreements reflect what is really an ongoing reality, which is that it takes time to resolve some of the issues, to comply with the recommendations. It would be helpful because in many cases these understandings or recommendations are undertaken with the agreement of the organizations, and it's just a matter of time.

The compliance agreements in the new bill would allow both them and us time to resolve the issue, but would still leave the door open if we need to proceed to court for enforcement.

● (1125)

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

Thank you very much, Mr. Carmichael.

We will now move on to Madam Sgro for five minutes.

Hon. Judy Sgro (York West, Lib.): We're glad to have you here.

I have a couple of questions.

How are Canadians going to be better off with Bill S-4? We know certainly some of them...front level, but I'm concerned with some of the other possible breaches and your ability as a department to pursue them.

Mr. Daniel Therrien: I think the requirement for that breach notification is a big part of it. The importance of this should not be underestimated. As I have said, and as we all know, breaches are a growing concern. With this requirement for organizations to advise both my office and individuals, we ensure, of course, that individuals are more regularly advised, and it will allow the office to analyze trends and to provide useful, practical, grounded advice to both organizations and individuals on how to reduce the risk of these data breaches. That's a big part.

Other than that, the compliance agreements will further enhance our ability to ensure compliance by organizations in a model without order-making power, but still it's a useful development to enhance these compliance mechanisms.

Consent is a big part of PIPEDA, and I think it's useful to have this clarification of what actually is consent. We obviously know that it is a huge challenge for organizations to properly advise individuals of the reasons they collect information and they use it, so any tool that enhances, that provides an incentive for organizations to be clearer, and to take into account the context of the individual or consumer I think helps Canadians.

Hon. Judy Sgro: How large a department do you have?

Mr. Daniel Therrien: We have approximately 180 employees.

Hon. Judy Sgro: Much of the data I see going through our various systems will often have “I accept the terms and conditions” and respect for this, that, and the rest of it.

Do you get a lot of complaints from people who didn't realize it, didn't bother to read the fine print, and expose themselves to being manipulated by the use of the data?

Mr. Daniel Therrien: Certainly, consent forms a significant part of the complaints we receive. Yes.

Hon. Judy Sgro: Is there a review in your office about how that could be clarified in a simpler way so people would know what they are consenting to when they say “I accept”?

● (1130)

Mr. Daniel Therrien: We've issued a number of documents that seek to inform both organizations. We have given guidelines to organizations on this matter and also to individuals, so that exists.

We're currently having discussions with stakeholders at the OPC in trying to establish new priorities for the next few years. One of the important themes mentioned by stakeholders during these meetings is although they think the OPC has played a useful role in providing guidance in this area of consent, overwhelmingly people are saying we should play a bigger role in education.

I take that advice, and certainly it's likely to be one of the things we want to enhance in future years.

Hon. Judy Sgro: The combination of C-13 and S-4, the impact of both of those pieces of legislation will be fairly significant, from what I understand.

Do you have any additional concerns over what you have mentioned specific to S-4 once those two are combined?

Mr. Daniel Therrien: I reiterate what I answered to Madam Nash, namely, yes, C-13 and S-4 on the issue of warrantless access to information create challenges and issues.

The decision of the Supreme Court in Regina v. Spencer is extremely useful and sets good parameters. I think it would be useful to go a step further and to further clarify lawful authority with a combination of the decision of the Supreme Court in Spencer plus a clarification of the circumstances where government can collect without warrant when there's no reasonable expectation of privacy. I think that would be a reasonable regime.

The Chair: Thank you very much, Commissioner. That's all the time we have.

We move to Mr. Daniel for five minutes.

Mr. Joe Daniel (Don Valley East, CPC): Thank you, folks, for being here. I have some fairly fundamental questions.

First, is there a clear enough definition for you to do your job in terms of what is considered private information versus what's already available in the public domain?

Mr. Daniel Therrien: One of the virtues of PIPEDA in my view is it is written in general terms, so it's conceivable that certain concepts like personal information, consent, or other concepts that are fundamental to PIPEDA might be further clarified. But on the whole I think it's better to have legislation written in general language, which allows for flexibility in application, a possibility to make the act relevant to various circumstances and to give practical advice.

Mr. Joe Daniel: Thank you for that.

To follow on that, numerous companies trade in data. What do you think the implications are to these sorts of organizations in terms of privacy?

Mr. Daniel Therrien: I think you're referring to data brokers.

Mr. Joe Daniel: That's right.

Mr. Daniel Therrien: That is clearly an area of concern. When individuals, consumers by and large, provide information to companies, they do so on the basis that they will receive a direct service from the company, and the agreement between the individual and the organization is information provided in return for a service.

Data brokers then collect information. They are not providing a direct service to the consumer. They are providing a service to other organizations. Individuals whose data is involved in many cases, if not in most cases, do not know of the existence of these activities, so this is clearly an area of concern that we need to pay more attention to and that other jurisdictions are paying more attention to.

● (1135)

Mr. Joe Daniel: In your introductory speech, you also talked about the determination of risk and the risk on the data that has been breached. You've put that responsibility on the person who actually created that breach, or should I say, that was breached. Is that correct?

Don't you think that allowing the people who have actually disclosed to decide whether it should be advised to you is kind of like putting the fox among the chickens?

Mr. Daniel Therrien: The first point I would make is that we can devise a breach notification regime in any number of ways. The one that you have in front of you is a good compromise. It's reasonable. Is there a better system conceivable? Probably. What I would ask you to do is to adopt that regime because the main point is we need mandatory breach notification.

Is it appropriate to leave organizations with the duty or the discretion to notify or not? In practical terms, we see that in Alberta, which has a similar scheme, but also federally with the voluntary breach notification that we've enforced for the past few years, organizations by and large do not under-report. They over-report. They want to report borderline cases because they don't want to be seen as under-reporting. Moreover, in Bill S-4, there will be penalties for those who under-report. Again, is this the best regime possible? Maybe, maybe not. I think it's reasonable overall and should be adopted.

The Chair: Thank you, Mr. Daniel.

[*Translation*]

Ms. Papillon, go ahead. You have five minutes.

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

When Minister Moore appeared before this committee a few days ago, I asked him whether the office would have sufficient resources and funds to accept the new and major responsibility that will follow once Bill S-4 is passed. He said that you had the resources you need for that.

Is that really the case?

Mr. Daniel Therrien: Clearly, we will do the work that we are required to do with the resources available. I said that this new obligation would lead to a major increase in our workload. In Alberta, the workload basically doubled when a similar mandatory notification system was adopted. The workload then levelled off in subsequent years, once the mandatory notification mechanism was adopted.

It would be premature to speculate on that, but we are pretty sure that the workload related to these notifications will increase significantly. In terms of the scope of the increase, we don't know.

I would suggest that we work with the resources we have, that we see how people respond and how many notifications we receive. After one or two years, we could see whether we need to allocate resources to that task.

Ms. Annick Papillon: When Ms. Kosseim appeared before the Senate committee, she also said that the issue of resources should be considered to its fullest extent because this new obligation will have an impact on resources.

Ms. Kosseim, do you have anything to add to that? The Senate committee does not always share what happens with this parliamentary committee.

Ms. Patricia Kosseim: In the commissioner's words, we will have to take a close look at this issue based on the experience we will have with the new system.

Ms. Annick Papillon: Very well.

Bill S-4 could force private sector organizations to report any losses or breaches of personal information. However, unlike what is set out in Bill C-12, the test proposed for this mandatory reporting is subjective since it enables the organizations themselves to determine, and I quote:

> if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.

In your view, is that test reasonable?

● (1140)

Mr. Daniel Therrien: As I said earlier, we can think of various ways of sending these mandatory notifications. The important thing is to have a system. At the end of the day, this seems to be a reasonable system.

Alberta's experience shows that companies and organizations provide notifications in many situations. In roughly half of Alberta's cases, the provincial commissioner notifies individuals of breaches that are reported by organizations, which seems to show that the organizations report to the provincial commissioner in borderline cases, when the scope of the harm done to an individual is not as clear.

Yes, there is a threshold after which the notification must be given. However, I think Alberta's experience shows that this is an appropriate way of doing things.

[*English*]

The Chair: Thank you very much.

Mr. Warawa, for five minutes.

Mr. Mark Warawa (Langley, CPC): Thank you, Commissioner, and witnesses here.

You said that requiring organizations to keep a record of breaches and provide a copy to your office upon request will give your office an important oversight function with respect to how organizations are complying with the requirement to notify. We also heard of the 45 days. If you are dealing with a complaint, or dealing with an organization where there's a privacy complaint, presently you have 45 days to take action in your enforcement. If you feel that you need to take action, the action would be going to the Federal Court. Is that correct?

Mr. Daniel Therrien: Yes. If we fear that certain conditions that we feel are necessary for compliance will not be respected by an organization, we have 45 days to seek redress in the Federal Court.

Mr. Mark Warawa: Right. That's your enforcement tool; you have 45 days to take action. You're working with the organization if there's a privacy concern, maybe a change of the privacy policies within that organization, but you have 45 days to take action. I think you shared that 45 days is not adequate time and in many cases you're looking at a longer time. You may give that organization six months to make changes, and if after six months they haven't made those changes—they said they would, in a hypothetical situation—45 days is past, and you have no more tools to take action against that organization, then extending the 45 days to one year would give you an enforcement tool that's very necessary.

Would you agree with that?

Mr. Daniel Therrien: Yes, it gives us flexibility to come to an agreement that makes sense with organizations on how to comply with the act.

Mr. Mark Warawa: Thank you.

The question came up in previous comments about consent. I'm thinking of changing technologies and data breaches. The world is changing as technology changes. We've heard recently about smart TVs that have voice recognition and people can make voice commands to a TV. If that function is on, do people really understand the consent that they've given to permit that, and what happens with that information? Is that information, the voices in the room, is that being put in text by a third party? What happens to that information? How important is it when people have given consent that they realize they've given consent?

Another part of the question of consent concerns children. Young children play games on tablets. Does a six-year-old or an eight-year-old understand the consequences of giving consent and providing their name, age, the town they live in, and their gender? What happens with that information? How important is it that there is understood consent that's given?

● (1145)

Mr. Daniel Therrien: We could spend a whole day on this issue of consent. Obviously, whether people provide consent with all knowledge of the consequences of their giving consent is a huge issue, and in many, many cases consumers, individuals, do not realize what they are consenting to. There's no question about that.

How does one ameliorate the situation? We think education is a big part of it. Guidance from the office is a big part of it for organizations and individuals. Is it possible to legislate this? The proposed definition of consent in Bill S-4 I think is a useful addition, but obviously you cannot prescribe all the potential situations where consent will be sought in the marketplace, so legislation has its limits. I think with the clarification that Bill S-4 provides, it is a useful clarification of what consent is, and it has the potential of improving the situation for the issue of consent sought from children, because the definition in Bill S-4 requires organizations to put themselves in the shoes of the individual whose consent is being sought: what does the individual understand? So, when the individual is a child, if your product is addressed to children, you should think about what is reasonable to expect of a child in understanding the consent being sought. Overall, I think, again, the definition of consent in Bill S-4 will assist generally and will assist particularly groups that are more vulnerable, like children.

The Chair: Thank you, Commissioner.

Ms. Nash now for five minutes.

Ms. Peggy Nash: I'd like to pursue the questions of Mr. Warawa around consent, because it is a topic that is certainly addressed in Bill S-4, and it's a very important topic that most people truly don't understand in an era of rapidly changing technology.

I discovered to my surprise that I ended up owning one of these TVs. It's a good thing I never get to watch it, but it apparently has the potential to be allowing someone to listen in. It would be pretty boring, but....

I wanted to ask you specifically about children. You did mention the consent of children. We're going to be hearing from the Chamber of Commerce, and they have said in their submission that your office has not been hampered in its efforts to protect children through ensuring valid consent; therefore, a specific valid consent amendment is not needed. What's your view on that? We'll ask this question also to the chamber, but do you believe that a specific valid consent amendment for children is needed?

Mr. Daniel Therrien: I would say that we have worked on complaints involving children, and we have been able to set certain parameters for how to obtain consent when the services provided by the organization are of interest to children, so it's not that we are currently without any tools to ensure the ability of consent generally and for children specifically.

That being said, I think it is useful to provide, to have the clarification that Bill S-4 proposes to have so that organizations see clearly from the definition of consent in what would be the new provision of PIPEDA, that they have to think about the clientele to which they're offering products and services. This probably is happening to some extent. Certainly it's happening to some extent for organizations, but it may not be happening for all organizations, and to have this clearly in legislation, that you must think about your clientele, I think would be useful.

Is it that are we without tools currently? No, but it would be useful to have this addition.

● (1150)

Ms. Peggy Nash: Thank you.

I have one last brief question. I think we've all been in a situation where we've gone to take an action online, and you are asked to read the terms and conditions. You click on it, and there are five pages of dense legal type. Those of us who are not lawyers, our eyes glaze over and so we are left with the question of what exactly we are consenting to. But if you want to conclude whatever transaction it is you're engaged in, you do consent even though you may not be fully aware of all of the implications.

Has the Privacy Commissioner and the commission explored the notion of plain language summaries or plain language translation of some of these legal documents, bearing in mind obviously that the legal contract is the binding one, but to get to the bottom line so that people fully understand what it is they're complying with?

Mr. Daniel Therrien: We have done that in the form of guidance to organizations, asking organizations to use plainer language when they seek consent. That's obviously only an incomplete answer, but at the end of the day, it is organizations that know the service they are providing and know what kind of information they need, so they're in the best place to inform consumers and individuals. We're urging them to use as plain language as possible.

That being said, consent is a huge concern. We think that Bill S-4 is a step in the right direction with the clarification to the definition found in it. But as I indicated before, we're consulting stakeholders on what our priorities should be for the next several years on how best to improve the situation for individuals. The consent that they provide will almost certainly be among our priorities.

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

Thank you, Ms. Nash.

Now our last questioner, Mr. Lake.

Hon. Mike Lake: Thank you, Mr. Chair.

Monsieur Therrien, there are three provinces with legislation dealing in the same area. Is that accurate? They are Alberta, B.C., and Quebec.

Mr. Daniel Therrien: Yes.

Hon. Mike Lake: Right. When you're dealing with your concerns, your reservations that you express on paragraphs 7(3)(d.1) and (d.2), my understanding, and you can correct me if I'm wrong, is that the new proposed legislation brings us far more in line with what's happening in Alberta and B.C. with what their legislation does.

Mr. Daniel Therrien: That's correct.

Hon. Mike Lake: That's correct, and that legislation has been place for how long?

Ms. Patricia Kosseim: I believe 2004 was when they were adopted, in that timeframe. For those specific provisions, I don't know offhand.

Hon. Mike Lake: Can you tell me if you're aware of any specific instances where there have been significant problems with the legislation as it's drafted in Alberta or B.C.?

Mr. Daniel Therrien: I'm not aware one way or the other whether they're having problems with these provisions.

Hon. Mike Lake: Just to be clear, that new legislation we're putting forward brings us more in line with those provinces, the legislation of those provinces, more consistent.

Mr. Daniel Therrien: That's correct, but as I've stated, the thresholds issue particularly makes me concerned that organizations would be able to share information for potential breaches or fraud cases that may not have materialized. That is a concern, a very real concern for me.

Hon. Mike Lake: Just to be clear, you're not aware that it has happened in Alberta or B.C.

Mr. Daniel Therrien: I have no information to that effect, no.

Hon. Mike Lake: Right, okay. Then you also mention, "However, if that is not possible, then I would recommend keeping the existing PIPEDA thresholds found in paragraphs 7(3)(d), and grounding disclosures in real problems rather than fishing expeditions". Then you have three bullet points.

It looks as though the changes that you're suggesting are very minor tweaks to what is being proposed in the legislation. Would that be fair to say?

● (1155)

Mr. Daniel Therrien: No, I would disagree with that. I think there is a fairly big difference between the proposed regime which would be authorizing organizations to share information for the purpose of investigating potential breaches versus the current regime where information can be shared only when an organization has reason to believe that there is a breach.

The difference is between investigating potential breaches or potential risk that a company thinks may be vulnerable to criminal activities, but without any evidence that there is such activity happening versus the current regime that requires reasonable grounds to believe that there is actually illegal activity occurring.

Hon. Mike Lake: When I look at (d.1) and (d.2) in relation to the suggested changes, (d.1) says, "is reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada". You use the quote "reasonable grounds to believe". It seems as though there is very little to choose between the two.

It's the same thing with your second bullet point where you also talk about "reasonable grounds to believe". I noticed you referred to a second quote that you would change to "has been, is being or is about to be committed".

In (d.2) it says, "is likely to be committed" in terms of the way the legislation goes.

Maybe specifically refer to what the difference is between them.

Mr. Daniel Therrien: "Likely" refers to a potential breach, so a breach that in the eyes of the organization is likely to occur but has not yet been seen.

Hon. Mike Lake: Similar to when I use my credit card one day in Edmonton, the next day in Ottawa, and the next day in Jamaica, there might be a concern by the credit card company that there might be fraud likely to be committed, so I might get a phone call. Because someone shared some information, I might get a phone call suggesting that there might be something up with my credit card. Is that right?

Mr. Daniel Therrien: At the end of the day, I think the difference is between allowing organizations to share for potential breaches not yet seen versus the current regime which requires that the breach has been seen or is occurring. There is a big difference in my opinion.

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

Thank you, Mr. Lake.

I wonder if I can make one small intervention because of the number of questions.

Mr. Lake referred to the fact that there is legislation in three provinces in regard to privacy. I know that Ontario has a privacy commissioner. Is there ongoing dialogue in regard to efficiency between the offices, overlap of legislation, ensuring that the best value for dollar, so to speak, is happening for Canadians and of course each resident of each province? Do you have a best practices meeting once a year?

I think the general public would probably want to know how you interact with the other offices.

Mr. Daniel Therrien: There is an annual meeting of federal and provincial privacy commissioners. We do work jointly on a regular basis. Guidance is often provided jointly so that there is consistency in what organizations receive.

So absolutely, we work in a very cooperative fashion with provincial commissioners, in part with a view to ensure greater efficiency.

The Chair: Thank you very much, Commissioner. I'm certain that all of my colleagues agree that we are very thankful for your testimony.

Colleagues, we will suspend while the next panel comes forward and then we will continue.

● (1155)

(Pause)

● (1205)

The Chair: Colleagues, we're back in session. We have before us two organizations.

The Canadian Chamber of Commerce is represented by Scott Smith, director of intellectual property and innovation policy.

Welcome, Mr. Smith.

Also before us is the Canadian Marketing Association, represented by David Elder, special digital privacy counsel. You'll see another name listed, Wally Hill. I've been advised that he may be bursting through the door at any moment; he's on a delayed flight. He is the senior vice president of government and consumer affairs. Mr. Elder will hold the fort while we're waiting for him.

We'll begin in that order.

Mr. Smith, would you begin your opening remarks, please.

Mr. Scott Smith (Director, Intellectual Property and Innovation Policy, Canadian Chamber of Commerce): Thank you, Mr. Chairman and members of the committee. The Chamber of Commerce appreciates the opportunity to address you on the subject of Bill S-4 and the changes that are proposed for the Personal Information Protection and Electronic Documents Act.

There has been much effort exerted in crafting this bill. As you're aware, there have been several iterations of it over the past few years. This is certainly not the first attempt at making changes to what is arguably the envy of other countries that are now just waking up to the principle of accountability.

This is principles-based regulation, and it provides guidance to business regarding their privacy obligations, avoiding overly prescriptive rules while at the same time permitting the necessary level of flexibility that leads to innovation.

In short, PIPEDA is a balance. Making legislative change without tipping that balance is a delicate matter. We would argue that the changes proposed in Bill S-4 are a successful attempt at maintaining the balance. The recommendations I'm going to be providing are very much procedural in nature and are not intended to fundamentally alter the spirit or intent of the bill. I'd like to characterize my comments as an opportunity to draw the committee's attention to specific provisions of the government's proposal that might benefit from targeted revisions that would align the changes to current industry practices while still meeting the government's objectives.

We support the objectives of Bill S-4 and the various proposed changes to PIPEDA that will bring some additional certainty and improvements to the overall PIPEDA framework, such as the new provisions regarding disclosure of personal information in the course of business transactions. These would broaden the scope of the exemption for business contact information to cover any information that is used to communicate or facilitate communication with an individual for business, employment, or professional purposes.

We are proposing targeted changes in four specific areas: one, valid consent; two, breach notification thresholds and record keeping; three, public disclosures; and four and perhaps most important, network information security.

The new valid consent provision in Bill S-4 denotes an obligation on organizations to pay particular attention to vulnerable individuals. While this is principles-based and broad in scope, the narrative around this provision has focused on specific categories of individuals. We see this as a concern for organizations that market broadly.

We also see it as unnecessary. I think you heard from the Privacy Commissioner this morning as well that this is a provision that, while he suggests it may be useful, isn't necessarily required. Section 5 of the act obligates every organization to comply with the model code, which is schedule 1. Section 4.3.2 of the model code says that for consent to be meaningful, “the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed”. In our view, this principles-based approach already captures the intent of Bill S-4, and we think the bill could be improved by simply deleting that clause.

The objective of notifying individuals in order to mitigate the risk of significant harm is quite different from the objective of notifying the Office of the Privacy Commissioner in order to catalogue breaches. This distinction is captured in the OPC guidelines from 2007 that define a real risk of significant harm and what constitutes a material breach. This dual threshold has been in practice for over a decade and is working well. In these cases there is no material breach, and the OPC reporting requirement would be onerous for both the organization and the OPC.

We encourage language that allows organizations to assess the risks associated with a breach and the OPC to issue guidance on what constitutes a material breach that triggers a reporting requirement, in other words, the existing regime.

Because there is no definition of what constitutes a material breach, record keeping is also problematic. Many occurrences, such as an unlocked filing cabinet with employee records, technically constitute a breach but have no material consequences. Keeping records in the prescribed manner for an unspecified time period when there is no impact on the privacy of an individual and the failure to keep those records constitutes a criminal offence is an unreasonable burden on organizations.

Also, with respect to what constitutes a material breach, we note that the compliance agreements should be directly linked to and focused on the requirements of PIPEDA to ensure transparency and clarity in the act regarding what companies must do to avoid finding themselves in a situation that might warrant a compliance agreement in the first place.

As drafted, proposed new section 17.1 raises concerns that overly broad language, for example, “any terms”, could result in potential jurisdictional overreach by the Privacy Commissioner. This limitation should be accompanied by a reasonable notice period.

● (1210)

Also, in clause 17, we are concerned that an exception to the general prohibition on disclosure granted to the Privacy Commissioner is out of step with other Canadian statutes, such as the Competition Act, and may have the unintended consequence of undermining current cooperative relationships and information sharing.

I've just spoken about the modifications we're recommending. We believe there's one very important omission in Bill S-4 that does warrant your consideration, which brings me to network information and security. The average number of days that a threat can reside on a network undetected is 229, and networks extend beyond individual organizations.

On February 13, President Obama issued an executive order calling for improved private sector cybersecurity information. This order recognizes that countering cyberthreats, private companies, not-for-profit organizations, executive departments and agencies of the government, and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible. We believe the same mechanisms are necessary here in Canada.

While proposals under Bill S-4 provide some limited exceptions to allow for collection, use, and disclosure of personal information, changes are needed to provide organizations with a legal certainty to effectively manage these threats. We are interpreting that network information security processing falls within the scope of PIPEDA since data processed for network information security purposes is often personal information like a name, an IP address of a botnet zombie computer, or an e-mail address. We are essentially asking for a clear-cut exception for network security information processing so that organizations have legal certainty and aren't forced to curtail network information security processing or operate in a legal grey area.

Our specific recommendations for text changes were submitted by the Canadian Chamber of Commerce on behalf of a coalition of businesses and organizations, and I urge you to consider those recommendations in the spirit of crafting the most effective privacy legislation.

Thank you for your consideration.

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

Now we move to Mr. Elder.

Mr. David Elder (Special Digital Privacy Counsel, Canadian Marketing Association): Thank you very much, Mr. Chairman.

Again, I'd like to apologize on behalf of my colleague Mr. Hill, who was delayed twice this morning on a plane. We all know what it's like travelling in this great country of ours at this time of year.

Thank you to the committee for the invitation to appear before you today, to comment on the digital privacy act, or Bill S-4.

The Canadian Marketing Association, or CMA, is the largest marketing association in Canada, with some 800 corporate members embracing Canada's major business sectors in all marketing disciplines, channels, and technologies.

The CMA is the national voice for the Canadian marketing community, and our advocacy efforts aim to promote an environment in which ethical marketing can succeed. With a few caveats, the CMA supports the government's initiative to update Canada's private sector privacy law. I should highlight two elements of particular importance to marketers.

First, the digital privacy act clarifies the definition of business contact information, so that electronic business addresses are treated in a manner consistent with that found in other privacy laws. This is an important and welcome change which businesses requested during the last review of PIPEDA.

Second are the breach notification provisions. During the last PIPEDA review, the CMA encouraged the Privacy Commissioner to develop national breach notification guidelines, which were issued in 2007, after consultation with stakeholders. The S-4 breach provisions build on those guidelines and will bolster consumer confidence that organizations will safeguard their personal information. This is especially important in 2015, when so much of our commerce occurs through digital channels.

We agree with the views and proposals presented by the Chamber of Commerce. I'd like to elaborate, however, on two of the issues addressed by my colleague.

First, proposed section 10.3 in the bill requires that organizations keep and maintain a record of every breach of security safeguards involving personal information under its control. This is of some concern, because the term “breach” is very broad, and there can be many technical breaches that could include any unauthorized access or disclosure of personal information no matter how mundane or non-sensitive.

There's no mention in this record-keeping requirement of a standard of materiality. All breaches will have to be diligently logged in a prescribed manner, even when there is clearly no risk. This could become an onerous obligation for businesses, especially for small and medium-sized businesses.

It creates several other challenges for organizations. There's the cost of gathering and storing that information. It also runs counter to good privacy practices to unnecessarily retain such personal information, especially for what appears to be an indefinite period of time.

Finally, one of the issues with this record-keeping concern is that it's one of the very few provisions in PIPEDA a violation of which constitutes an offence over the act. Consistent with what Mr. Therrien said this morning about how businesses have approached reporting breach notifications, I think you will also have a situation here in which we may have overcollection because businesses want to be onside with the law. As well, a great deal of effort and material will be spent cataloguing very minor breaches.

The CMA recommends that a materiality threshold be introduced as outlined in the business coalition brief. At a minimum, it's very important that the materiality threshold and retention period be addressed, first with a reference in the law, and then possibly through a more detailed regulation.

The second issue I'd like to talk about is clause 5, which proposes a new section 6.1, which elaborates on the definition of what it means to obtain valid consent. The minister has explained that this clause is intended to reinforce existing best practices, to protect certain groups, such as children, who may have more difficulty understanding privacy and related consent language.

Incidentally, the CMA has long required that its members afford special consideration for young people. The OPC, has also noted favourably how the CMA code of ethics and standards of practice puts in place special consent provisions for the collection, use, and disclosure of personal information from children and teenagers for marketing purposes.

However, in addition, the OPC has already, under the existing wording, issued decisions requiring that extra care be exercised to ensure that young people understand an organization's privacy practices, and has further produced guidelines indicating that organizations should recognize and adapt to special considerations in managing the personal information of children and youth.

● (1215)

There's a presumption, as you would well know, in statutory interpretation that each provision is supposed to do something. It's often said that the legislatures don't speak in vain. The question here is, what does this new provision do? If we already have a provision that requires generally that individuals understand what their information is being used for and give consent based on that knowledge, what additional does this do?

I think the concern here is that the clause, as written, could lead to a broad interpretation with additional obligations. We've heard that the concern is about children and vulnerable groups. However, that's not what the bill says. It's much broader than that, and we would like some clarification of that bill.

Actually, our recommendation would be to drop this clause or, as a fallback, to amend it to clarify that it is intended to apply only to vulnerable groups.

Canadian marketers and the CMA fully recognize that consumer confidence is of paramount importance and that respect for personal information is a key ingredient. The preamble to PIPEDA states that the law is intended to promote electronic commerce by protecting personal information. Sound privacy protection practice is good for consumers, good for businesses, and good for our economy.

We thank the committee for its attention and would be pleased to answer any questions you might have.

The Chair: Thank you, Mr. Elder.

Colleagues, there is another committee coming in here afterwards which I'm very familiar with, as I mentioned to you before, so we'll have to stay pretty tight to times. Witnesses and colleagues, please forgive me if I cut you off, we have to stick to four minutes.

I'll begin with Mr. Lake.

Hon. Mike Lake: Thank you, Mr. Chair.

Thank you to the witnesses for coming.

You both brought up section 6.1. I am really interested because as I read this, it sounds pretty straightforward. I can't imagine that most Canadians looking at this would have too much trouble with the wording. I'll just read it because it's not very long.

> 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 of the collection, use or disclosure of the personal information to which they are consenting.

I don't really understand the hesitation from both of you regarding that kind of language. I think most Canadians would expect that a user taking a look at a website or signing up for an organization's activities would be able to understand what that information is going to be used for.

● (1220)

Mr. David Elder: Thank you for that question, Mr. Lake.

The concern is that we already have language in the law which says that to make a consent meaningful, the purposes must be stated in such a way that the individual can reasonably understand how the information will be used or disclosed. What we're trying to understand is what additional requirement is being proposed under this consent, particularly given that we've already had decisions out of the OPC and guidance issued particularly about vulnerable groups.

The concern is, how far does this go?

I think the industry accepts, particularly when you're dealing with children and youth, that you need to have privacy policies worded in such a way that they would be reasonably understandable by that audience.

But how far does it go? If I have a multitude of sites, and for operational reasons I'd obviously like to have a single privacy policy for each one, how granular do I have to be? If one of my sites is directed at hockey fans, do I have to do survey research to tailor that to hockey fans because they might have a different way of understanding the way things are presented? If I'm a game manufacturer and I have a role-playing game and I have something like Candy Crush and I also have a word game, do I have to have something different for each of those? I think this is what we're concerned about.

Hon. Mike Lake: Actually, yes, you do.

Quite honestly, if your target market in one of the situations is adult hockey fans and your target market in another situation is eight-year-old kids you should have a different approach.

Mr. David Elder: Exactly. But if your target market is adults in both cases—

Hon. Mike Lake: Then you should be fine.

Mr. David Elder: —adults who you have no reason to think are any different but have different characteristics, they are a different target market, how far do you have to go? I think that has been the concern.

Hon. Mike Lake: How far do you have to go? You have to go to the point where the person would understand the nature, purpose, and consequences of the collection, use, or disclosure of the personal information. That seems pretty clear.

The Chair: Very briefly, Mr. Smith.

Mr. Scott Smith: I think the second part of that question is, what constitutes vulnerable? It's not defined in the act.

Hon. Mike Lake: So?

Mr. Scott Smith: Okay.

Well, the other side of it is the number of instances where you have that also for companies that target broadly. For instance your social networking sites that would target everybody need different policies to be able to appeal to different people.

Hon. Mike Lake: They're gathering information; one would hope they know who they're targeting

Mr. Scott Smith: But they're targeting everybody.

Hon. Mike Lake: Well, then, you know what? Everybody includes kids, and if they're not going to differentiate, I guess they have to make everything easy enough for an eight-year-old to understand.

The Chair: That's all the time you have.

We will now move on to Ms. Nash.

Ms. Peggy Nash: Thank you, Mr. Chair.

I'm just trying to get clear in my mind this discussion about consent.

We've heard from both of you that this presents a challenge. You've said that it's a hardship, and that it costs businesses to be compliant. You've also said that it's unnecessary because the Office of the Privacy Commissioner is currently able to ensure valid consent of minors, and that industry best practices are high enough to protect minors, as well as other groups.

If it is the case that the current provisions are adequate, and if you're convinced that this change, which the commissioner says is useful, is not going to change much, why is there any additional cost associated with it? How can it possibly be a hardship if you're saying it's not doing anything?

● (1225)

Mr. David Elder: I guess the assumption is that it must do something, otherwise Parliament would not enact such a provision.

Ms. Peggy Nash: The commissioner believes it will do something. He believes it will go down the road another step—I think that was how he put it—to securing better knowledge of consent, and a more meaningful consent.

Mr. David Elder: I'm not really seeing how that would work. Again, the wording currently says that you have to state purposes in such a manner that the individual can reasonably understand how the information will be used or disclosed. The wording now says similar things; it says, "would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information".

Ms. Peggy Nash: My question for you is, if that's the case, where is the problem?

Mr. David Elder: What I would say is, if this doesn't do anything, then there's no reason for it to be here.

Ms. Peggy Nash: You're saying it's superfluous.

Mr. David Elder: If it is here, I'd like to better understand what it does that's different from what we already have, where we already have this requirement that the individual needs to understand the purposes, and where we already have guidance from the OPC about how to treat children, for example, and other disadvantaged groups.

Ms. Peggy Nash: Perhaps it just formalizes the guidelines you say industry is already following, and codifies them in law in a way that adds greater clarity. The commissioner believes that it adds greater protection. My question is whether it's either a burden and a hardship or whether it does nothing. I have trouble understanding that it's both a burden and a hardship to business, but that it doesn't do anything in this case. The commissioner says it is helpful; it is another step in providing meaningful consent. To me that's a worthy goal. I'm trying to understand what is the undue hardship to business that suddenly will transform the way business behaves.

The Chair: Briefly, please.

Mr. David Elder: Again, part of it is that we don't really know. If it is a clarification, it might be useful to have a revision that says "for greater certainty", or something like that to indicate that we are just trying to clarify an existing obligation. Our concern is what this means additive to what's already here. If it doesn't do something additive to what's already here, there's no reason to enact it. That's how a court would interpret this.

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

Now Mr. Carmichael for four minutes.

Mr. John Carmichael: Thank you, Chair, and welcome to Mr. Hill as well. Your travels finally got you here.

I'd like to refer to the commissioner's comments earlier about the number of breaches that are becoming commonplace, and as he said, becoming a growing phenomenon. He's approximated at 60 a year the number of breaches that are being declared at this time. That's up or down a bit, but that's going to continue to grow with mandatory notification.

Mr. Smith, I would like to start with you directly, and then go to Mr. Elder. I wonder if you could give me some examples within your community, within the chamber, and within its membership, of what businesses are doing to take action today, to comply with this legislation that's coming forward.

In terms of protecting against such breaches, how are businesses getting ready for this type of phenomenon?

Mr. Scott Smith: There are a couple of ways to answer your question.

The legislation has been in place for over a decade now and it's working well. As you heard, businesses are reporting.

There are incidents. These breaches are increasing. You hear about them in the media. Generally, those are not the fault of the businesses. They're being attacked in a number of different ways. If you're talking from a cybersecurity perspective, they have challenges in being able to protect themselves against that. That's not unique to business. That's happening to government. It's happening to everybody. You heard that even the U.S. government was attacked.

From a small business perspective, they look at PIPEDA and are doing what they can to comply. Most of the breaches that you don't hear about are being handled at the front lines and reported to individuals. It's not coming back to the Privacy Commissioner at all. Generally there's no need for it to come back because there is no risk of harm to that individual once the breach has been dealt with. Systemically, they're managing these internally.

Is business preparing for the changes to PIPEDA that are coming under Bill S-4? They're certainly aware of them. Will they make any changes? Not until the bill comes into place, I would suspect.

● (1230)

Mr. John Carmichael: Are the changes significant to small business?

Mr. Scott Smith: To small business, probably less so. To large businesses, they will be significant, particularly as I mentioned the ones that are targeting large numbers of different classes of individuals.

Mr. John Carmichael: Right.

Mr. Elder or Mr. Hill, do you want to comment?

Mr. Wally Hill (Senior Vice President, Government and Consumer Affairs, Canadian Marketing Association): Yes, thanks.

To reiterate in a little more detail, Scott is correct in highlighting that the law has been in effect for over a decade now. It's an ongoing process. Organizations are constantly upgrading their security procedures and practices, and their technology. All of us are reading about technological changes every day, and those pose new challenges for marketers and for businesses every time there is a significant development. Businesses need to stay on top of their game, and they work constantly to do so. They have been doing that on the basis of PIPEDA since the early 2000s.

In terms of small businesses, the only thing I would add is that there are elements of the law that present concerns to us. I missed the introductory remarks, but with regard to the record-keeping requirements, for example, there is some concern that if they're not qualified a bit more, that could pose a burden for businesses generally, but particularly small businesses, in terms of having to keep records relating to a breach.

The Chair: We're over time and we have to stay pretty strict. There is another committee coming in afterwards.

Ms. Sgro, for four minutes.

Hon. Judy Sgro: Thank you very much, Mr. Chair.

Welcome to our guests.

The whole intent is on how we better ensure through Bill S-4 that Canadians are protected and that the appropriate law enforcement and so on have the tools they need to do their jobs. I think that's what everybody wants to see happen. Whether Bill S-4 accomplishes that or not is fully questionable.

Mr. Smith, you mentioned the issue of network information security in particular . Would you elaborate a bit more on that?

Mr. Scott Smith: There are provisions under clause 7 that provide exceptions, for example, for protecting for fraud, and it was discussed in the previous session. There is no provision to manage a cybersecurity hack, for instance. An example is the Waledac. It was a botnet that attacked large numbers of computers, and it had the ability to send 1.5 billion spam e-mails a day. The only way to counteract that is to collect information from those computers that are hacked and then provide advice to those individuals on how to solve that problem. It has to happen in a fairly short period of time; you wouldn't have time to collect the consent to do that. For businesses to operate and share information and collect information in real time, they do need some kind of exception to operate.

Hon. Judy Sgro: Does anybody else want to comment on that?

It gets very complicated and difficult. Government today has one intent here, and it's to make sure that people are protected. You looked at consent. You have seven-year-olds and probably even four-year-olds with iPads and they want to keep that gas going and they'll be hitting “I accept”. They don't read it; they don't care about it. They're just accepting it and they're fully exposed in having allowed that consent.

How do we better protect the consumer? That's what I want to make sure of. You've mentioned some amendments on other ways, but I think that consent issue is a really important one when you talk about new immigrants to Canada who are not completely familiar with the English language. People are accepting; we as parliamentarians are not reading the "I accept" thoroughly, and let's be honest about it. We're all busy; it's just going to be the normal stuff. We want to make sure we're making that safer and better so the consumer and Canadians are better protected.

You seem to be more concerned with the impact it's going to have financially on businesses, which I understand as well, but we want to be able to do both.

● (1235)

Mr. Scott Smith: If I could just go back to the cybersecurity issue for one moment, the whole intent of that requested amendment was to protect consumers and individuals. In other words, it's those consumers and individuals whose information is at risk, and we're just suggesting that to be able to handle that it's not in their best interest to ask for their consent in the first place. It's in their best interest to handle the problem.

Mr. Wally Hill: I would hearken back to the minister's comments a week or so back when he was talking about proposed section 6.1 being designed or intended to better protect the especially vulnerable groups, particularly vulnerable groups in society such as children, and I think that is an important objective of PIPEDA. Many experts believe that PIPEDA has built into it now the provisions that allow the Privacy Commissioner to specify the forms of consent that are needed in specific circumstances relating to children or adults.

I would also point out that a combination of best practices and self-regulatory regimes is out there in the marketplace, as well as PIPEDA, that helps to protect certain groups. Our own code of ethics embodies provisions specifically designed to protect children, especially those under 13.

The Chair: Thank you, Mr. Hill.

We're over time again; I apologize that I have to intervene a second time. Somebody asked Mr. Hill a question up front and I didn't want to interrupt him again.

Mr. Daniel, you have four minutes.

Mr. Joe Daniel: Thank you, folks, for being here.

I was listening intently to all your discussions and there were a couple of terms that I didn't fully understand. Mr. Elder, you talked about overcollection. What is this overcollection? Why is it being collected, and what's the purpose of it?

Mr. David Elder: Thank you for the question.

The overcollection I was referring to was, I think, a likely outcome of proposed section 10.3 in the bill that requires organizations to "keep and maintain a record of every breach of security safeguards involving personal information under its control". Personal information is a very broadly defined term. It's really any information about an identifiable individual and there can be frequent small breaches, technical breaches happening every day. I will give a couple of examples. Let's say a misprinted address label goes out in the mail that includes in the address window the party's age. That's a breach, a piece of personal information tied to an identifiable individual. Let's say you're in a store and the clerk leaves somebody's order printed out on the counter while he turns to get the phone and it's visible to other consumers and all that may have been disclosed was somebody's shoe size. That's a breach. A record would have to kept for each of them under this law and retained indefinitely until the OPC requested it.

I think that's our concern, that there's no threshold here of materiality and I think because of the concern that this provision is tied to an offence provision, there will be overcollection. Businesses will err on the side of caution and will record everything in all the stores and all the call centres everywhere across the country.

Mr. Joe Daniel: That's your interpretation of the bill as it stands. That's kind of your definition as well, which brings me to my next question, which is about what was considered a minor breach. You're basically saying it's a breach that doesn't impact anybody. Is that what you're saying?

Mr. David Elder: Yes. I think we already have standards in this bill and in previous bills that could be helpful in terms of talking about, for example, we think it's certainly reasonable to keep records if it's reasonable that the breach would create a real risk of significant harm to an individual.That's already proposed for notification of individuals and the Privacy Commissioner. I think that would be a good standard in terms of materiality for the record keeping required. You'd know that they meant something and there was some real risk of harm.

● (1240)

Mr. Joe Daniel: This question is for both organizations. Are you actually collecting data relating to the impact of some of the bigger breaches? We're not talking about these minor ones now. What is the financial impact on the organizations that have been breached? What are the financial implications to those whose information has been breached? Is there any tracking of that so we have some measure of what's going on?

Mr. Scott Smith: To answer that question, yes, that's part of any company's process in evaluating a breach: what is the impact of the breach? They all have internal policies on how to manage that. Financial institutions would have a very rigorous set of policies, whereas a small business may have something very straightforward, depending on the type of information they collect.

The Chair: Thank you very much.

Now on to Ms. Papillon.

[*Translation*]

You have four minutes.

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

Bill S-4 can force private sector organizations to report any losses or breaches of personal information. The test proposed for this mandatory reporting is subjective since it enables the organizations themselves to determine whether it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.

In your view, can we ask organizations to determine themselves what constitutes significant harm? Would that assessment not be too subjective? What do you think about that?

[*English*]

Mr. Wally Hill: Individual organizations have a lot at stake in terms of ensuring that they properly weigh the impact of any breach on their customers. Their most important assets as business organizations are their customers, so making that sort of evaluation is one of the most important functions an organization has to take on when there is a breach situation. They are in the best position to evaluate the level of risk to their customers, and then to take appropriate action.

I believe that the law as drafted largely has that component constructed in an appropriate way. There is provision for reporting also to the Privacy Commissioner, which is an additional component that supports, I guess, the safeguards under the new provisions of the law.

Mr. David Elder: If I could add to that, I would say that the other thing working here is that in all cases, this is being overseen by the Office of the Privacy Commissioner. At first instance, a business may make the call as to whether something creates a significant risk of harm, but ultimately that will be up to the OPC to review at some point, or a court, and if organizations get it wrong, that's an offence under this act. They're subject to fines on summary conviction, so there's a lot of incentive there for them to get it right.

[*Translation*]

Ms. Annick Papillon: The organizations don't necessarily agree on what a real risk of significant harm is. In your view, will the standard proposed lead to under-reporting or over-reporting of the breaches identified by those organizations?

[*English*]

Mr. Wally Hill: I would suggest that it will lead to an appropriate level of reporting, and reporting those breaches that should be reported both to the Privacy Commissioner, and most importantly, to affected consumers.

Mr. David Elder: I think, as we heard from the Privacy Commissioner himself this morning, the experience with the breach of reporting regime in Alberta and with the voluntary regime in the rest of Canada shows that companies are tending to over-report.

[*Translation*]

Ms. Annick Papillon: Actually, we heard this morning that, in Alberta, the workload doubled overall. That will certainly affect the resources. It is a good reminder.

Clause 24 of Bill S-4 is amending section 28 of PIPEDA. It says that every organization that knowingly contravenes the new provisions of PIPEDA, which require organizations to report security breaches and to retain that information, or that obstructs the commissioner in the investigation of a complaint or in conducting an audit is guilty and liable to a fine not exceeding $100,000 for an indictable offence and not exceeding $10,000 for an offence punishable on summary conviction.

In your view, are there any indications that the risk of a fine of up to $100,000 could help enforce the law?

● (1245)

[*English*]

The Chair: Sorry, Ms. Papillon. We went over during your question, so if somebody wants to answer it during another round, you can do that.

Mr. Warawa, for four minutes.

Mr. Mark Warawa: Thank you to the witnesses.

The Canadian Chamber of Commerce and the Canadian Marketing Association, did either or both of your organizations make submissions to the Senate hearings in dealing with S-4?

Mr. Wally Hill: The Canadian Marketing Association did.

Mr. Scott Smith: We did not.

Mr. Mark Warawa: Legislation can begin in either the House of Commons or the Senate, so S-4, because of the "S" in front of the number instead of a "C", indicates it began in the Senate.

Mr. Smith, is there a reason that the Canadian Chamber of Commerce did not make a submission in the Senate?

Mr. Scott Smith: Mostly it was trying to come to a consensus among our members. We had narrowed the number of issues we had with this from probably 30 down to the four that you saw on our submission. It took a significant amount of time to do that, and we were looking at things that would be most supportive as we could make it, which is why we didn't meet the deadline for submission to the Senate committee.

Mr. Mark Warawa: Mr. Smith, you said you wanted to consult with your members. What percentage of your members did you consult with to come up with these positions?

Mr. Scott Smith: I honestly couldn't tell you what the percentage is.

Mr. Mark Warawa: Okay. Thank you.

You said there would not be much of an impact on small business, that the large impact of breach reporting would be on large business. I think we heard the opposite from the other presenters. Do you still agree with that?

Mr. Scott Smith: I think the caveat in there is on the record keeping, that small businesses probably have less capacity to manage the record-keeping obligation than larger businesses do, and in crafting their policies those small businesses probably are going to be looking to organizations like us to help them with these changes.

Mr. Mark Warawa: So you would agree that record keeping would be a bigger impact.

Mr. Scott Smith: Yes.

Mr. Mark Warawa: Are most of your members small or large?

Mr. Scott Smith: So that you understand the structure of the Canadian Chamber of Commerce, we have direct memberships from corporate Canada—all of the companies you would recognize. Fortune 500 companies are direct members. Indirectly we represent small business through our chamber network. We have 450 chambers of commerce across the country. Those small businesses generally belong to those local chambers.

Mr. Mark Warawa: The reason I ask is I'm a member of a very active chamber in Langley, and I did not hear this come up, so I was surprised that the position was opposing S-4.

Maybe you want to clarify that.

Mr. Scott Smith: Yes. We certainly don't oppose S-4. As I said in my opening statement, we're suggesting there are a few targeted changes that could be beneficial, but by and large we certainly support S-4.

Mr. Mark Warawa: Good. I appreciate that clarification.

The commissioner said PIPEDA is written in a general language to allow flexibility so if there was contradiction, a breach, and inadequate reporting, if there's a complaint lodged, then it would go through the Privacy Commissioner. He or she would look at it, and at this point he has 45 days to take an action. S-4 is suggesting that change to a year.

Would you agree with that proposed change?

The Chair: A quick response, please.

Mr. Wally Hill: Yes, I think we would agree that added period of time is helpful to the commissioner.

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

[*Translation*]

Ms. Papillon.

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

Mr. Smith, let me then go back to the question that you were not able to answer, namely whether there are any indications that the risk of a fine of up to $100,000 will help enforce the law.

[*English*]

Mr. Scott Smith: I can't say that it will help with the enforcement of PIPEDA. There is a high degree of compliance with PIPEDA as it stands right now. I don't see that changing with Bill S-4 in our understanding of the offence provisions that are included in Bill S-4. They are intended to deal with the most egregious infractions where there is a deliberate contravention of the act.

● (1250)

Mr. Wally Hill: I would agree with that. Having the penalties in the act does provide some additional teeth to the law that will get the attention of those who maybe need to pay closer attention to their privacy obligations. But for the most part, as Mr. Smith indicates, the business community increasingly has been understanding the importance of privacy and its responsibilities in terms of adhering to the requirements of PIPEDA.

The Chair: You have two minutes.

Ms. Peggy Nash: Thank you, Mr. Chair.

In terms of the issue that has been of concern to this committee about warrantless disclosures and the concern, for example, that the recent Supreme Court decision may require amendments to Bill S-4 as it currently stands, how has business been handling this concept of warrantless disclosure and the sharing of information without the knowledge of the individuals up until now? I presume it hasn't specifically been permitted. Has that been a problem? In other words, has it been business saying the issue of not requiring consent is a problem we need to address?

Mr. David Elder: I'd preface my remarks by saying I'm not sure this is really an issue that the Canadian Marketing Association is pushing. That being said, I wear other hats, so I would say that the practice is a bit mixed across the country with regard to voluntary disclosure to law enforcement. There are a number of service providers, for example, that absolutely refuse to give anything to law enforcement without a warrant.

Ms. Peggy Nash: Do you mind if I clarify my question? What is the problem that this change in Bill S-4 is trying to fix?

Mr. David Elder: I think that is probably one that's better put to the drafters who know the law, frankly.

Ms. Peggy Nash: Mr. Smith, of the people you represent, have any businesses been saying this is a change they want?

Mr. Scott Smith: As far as I understand it, there is an interest from the insurance industry on this with respect to cases of fraud. It makes it easier for them, and as you heard this morning, it changes the investigative bodies regime, which allows them to go through the process without going through the process.

Ms. Peggy Nash: Thank you.

The Chair: Thank you, Ms. Nash.

Mr. Lake.

Hon. Mike Lake: I want to follow up on some comments from the original opening statements.

We have this threshold of real risk of significant harm and, Mr. Smith, you referred to that: an organization determines that there's a breach that poses a real risk of significant harm, and they have to report it to their clients, the people who are affected by it, but you would suggest that they need not notify the Privacy Commissioner. You don't think they should have to notify the Privacy Commissioner.

Why, if it is a breach that is significant enough to pose a real risk of significant harm, significant enough that they would take the step of notifying their own clients, people who are affected by it, would they not have to notify the Privacy Commissioner?

Mr. Scott Smith: The process to date has always been a two-step threshold. There were several examples mentioned this morning. There could be a name wrong on a letter in an envelope, or there could be a phone number posted somewhere that wasn't supposed to have been posted. The decision often gets made at the front-line staff or the customer service staff, that you deal with the individual. You let people know what happened and let them know what you're doing about it, but is there—

Hon. Mike Lake: This is real risk of significant harm.

Mr. Scott Smith: Right. We're concerned that the way the bill is drafted, that from the over-reporting perspective, if you have to send every single one of those to the OPC, it significantly changes the number of records that you're going to have, the number of records that the OPC is going to have.

Is there any real value in reporting that? Probably not.

Hon. Mike Lake: Most Canadians would say probably and disagree with that when there's a real risk of significant harm.

When there's not a real risk of significant harm, though, the legislation says we're not going to make you report everyone to the commissioner, but we are going to make sure that you track the error.

Again, when I look at proposed section 10.3—everybody's brought up issues with this—it's pretty straightforward. It says that you have to "in accordance with any prescribed requirements, keep and maintain a record". But you only have to keep and maintain a record for every breach of security safeguards involving personal information under your control.

Basically, you're only keeping records when you make a mistake that involves someone's personal information. The amount of information that you have to track, the amount of cost associated with this is in direct correlation with the number of mistakes you make in tracking people's personal information. Is that a problem?

● (1255)

Mr. Wally Hill: Because of the language in the bill, there is not really a threshold established. It just says, "any breach of security safeguards involving personal information". That could be something as minor as a list of addresses being left out, something very, very minor in the historical context of personal information under PIPEDA. The law appears to indicate that those pieces of information will then have to be logged, recorded, and kept for an unspecified period of time.

Hon. Mike Lake: Actually no, there's a consultation process. You guys know that there's a consultation process that you'll be able to weigh in on to say what that's going to look like.

Who knows, in the end it might be as simple as an e-mail trail saying what happened filed electronically to ensure that in the future it can be looked at. It doesn't seem that onerous to me in this day and age of computer technology

The Chair: Mr. Hill, you have the final word.

Mr. Wally Hill: Our concern is that it could be taken to extremes and we haven't seen the regulations. You're correct. We'll have an opportunity to sit down in that process and one would hope the outcome would be a reasonable framework that wouldn't impose too great a burden.

Our concern was simply that there could have been some mention of threshold in the law and that would have given reassurance to business.