HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

# Standing Committee on Industry, Science and Technology

INDU • NUMBER 035 • 2nd SESSION • 41st PARLIAMENT

**EVIDENCE**

## Thursday, February 19, 2015

---

## Chair

**Mr. David Sweet**

# Standing Committee on Industry, Science and Technology

**Thursday, February 19, 2015**

● (1130)

[*English*]

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

Welcome to the 35th meeting of the Standing Committee on Industry, Science and Technology.

I have a little bit of clairvoyance regarding votes; I think we may be called out again. So I think it's most urgent that we try to get your testimony on record first, because we may be interrupted.

I understand, Ms. Nelson, that you need to leave by noon. Is that right?

**Ms. Jean Nelson (Honourary Executive Member, National Privacy and Access Law Section, Canadian Bar Association):** Yes. Thank you.

**The Chair:** Then why don't we begin with the Canadian Bar Association.

Please give us your opening remarks.

**Ms. Jean Nelson:** Thank you very much, committee members. My name is Jean Nelson, and I'm a member of the executive of the Canadian Bar Association's national privacy and access law section. I'm also a member of the Canadian Corporate Counsel Association's advocacy committee.

With me is Suzanne Morin, who is also a member of the national privacy section's executive.

Thank you very much for taking the time to hear from us today, especially on a very busy day. The CBA, as you might know, is a professional association of 36,000 lawyers. We represent a diversity of organizations, not-for-profits, members of the private bar, and corporate counsel. Our mandate includes upholding the rule of law in the administration of justice. It's from that perspective that we come to you today.

We want to speak in support of the objectives of Bill S-4, but we wish to also make some recommendations. Our recommendations are offered in the spirit of ensuring greater clarity for Canadians, Canadian businesses, and Canadian organizations. I am conscious of the time, so I will highlight two aspects of our written brief, which you should have before you. I will highlight disclosure without consent, and my colleague Ms. Morin will highlight breach notification. We'd be pleased to answer questions about any aspect of our brief.

First I will speak to disclosure without consent. We believe, in a nutshell, that this provision should be subject to further analysis in order to consider narrowing its scope. We are concerned that, as drafted, it's unnecessarily broad and will permit disclosure without consent in an inappropriately broad range of circumstances.

These new sections appear connected to the removal of the concept of investigative bodies from PIPEDA. You might recall that under that investigative body scheme, the Governor in Council could approve by regulation specific bodies or categories of bodies to which organizations could disclose personal information. These proposed new sections are consistent with CBA's position on this issue as expressed earlier, when it urged the government to consider the models used in Alberta and British Columbia. However, in our perspective, it doesn't quite hit the mark. We believe it requires finesse, as we said in our written brief. We would be pleased to work with Industry Canada and other stakeholders to achieve the appropriate balance.

We understand the need for the proposed additions, as major industries in Canada, such as banks, financial services, and other private sector organizations, need to share information to detect, suppress, and investigate fraud. We are of the view, however, that this provision should be more closely tailored to its actual purpose to prevent abuse of its broad wording.

Mr. Chair and committee members, that concludes my remarks. With your permission, I'd like to now invite Ms. Morin to amplify the CBA's perspective on breach notification in Bill S-4.

**Ms. Suzanne Morin (Executive Member, National Privacy and Access Law Section, Canadian Bar Association):** Thank you, Jean.

I will limit my opening remarks to just two areas regarding the breach notification regime. The first one is thresholds for reporting to the Privacy Commissioner, and then the second area will be record-keeping.

As you may know, unlike its predecessor, Bill C-12, clause 10 of Bill S-4 sets out a single test or threshold for both notifying individuals of a breach and reporting to the Privacy Commissioner. In effect, every breach that is notifiable to an individual will now also be reportable to the OPC, requiring businesses to change their current practices. The objective of reporting to the commissioner in essence is to track the volume and nature of breaches to see if there are any trends and to allow the commissioner to work with organizations, small and medium-sized organizations, who may need assistance.

This objective is very different—very different—from the objective of notifying individuals so that they can mitigate harm that may result from the breach. This distinction is actually very well understood both by industry and by the Privacy Commissioner's office. In fact, industry players have been following for years the guidelines “Key Steps in Responding to Privacy Breaches”, which were jointly issued by the Privacy Commissioner with their B.C. and Alberta counterparts. These guidelines have existed for several years and have been followed by the industry very successfully. While the threshold for notifying individuals should be based on the existence of a real risk of significant harm, which is what Bill S-4 does today, reporting to the OPC should be premised on the existence of a material breach.

Second, regarding record-keeping, we are of the view that the mandatory record-keeping for all breaches of security safeguards regardless of significance is unworkable, extremely impractical, and places too great a burden on all organizations regardless of size or industry, with no commensurate benefit for the protection of Canadians. In fact, this is really our overarching concern when these new record-keeping obligations are considered in light of the new proposed offences which, in our view, strip away the delicate balance in PIPEDA. In no event should a deficiency in logging be an offence.

As currently drafted, and due to the lack of a specific materiality threshold for reporting breaches to the OPC that I just referred to, every single breach of security safeguards, once again regardless of how trivial, must be diligently logged because it will be an offence to do so improperly or imperfectly.

In closing, we should be focusing on those breaches of security safeguards that might have the most impact on Canadians.

Once again, on behalf of my colleague and me, thank you for the opportunity to meet with you here with today, and we welcome your questions.

● (1135)

**The Chair:** Thank you very much, Ms. Morin.

Now we'll move on to Mr. Israel.

**Mr. Tamir Israel (Staff Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic):** Thank you, Mr. Chair, and committee members.

My name is Tamir Israel, and I'm a staff lawyer with CIPPIC, the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, at the University of Ottawa. CIPPIC works to advance the public interest in policy debates that arise at the intersection of law and technology. We're very grateful for this opportunity to provide our input into Bill S-4, the digital privacy act, which will make some important changes to PIPEDA, Canada's federal commercial sector privacy law.

Concern over privacy and lack of trust in organization practices remain an ongoing concern for a number of Canadians. A recent survey commissioned by the Privacy Commissioner found, for example, that over 75% of Canadians have avoided the use of a mobile application because of the information requested, and close to 60% have turned off location tracking functionality on their mobile devices out of concern that others will access the information. These types of statistics are telling, and they show that Canadians remain concerned, and are acting on their concerns, when engaging with digital content.

Even as concerns grow, avoiding privacy-invasive practices becomes increasingly difficult. Every device, from our mobile phone to our car to our television at home, is now a cause of concern for those wishing to maintain a sphere of privacy. The task of keeping up with the multitude of settings and privacy policies on all of these is time-consuming, and increasingly out of reach for many segments of the digital population.

Against this backdrop, Bill S-4 introduces some much-needed improvements to PIPEDA, while at the same time raising some concerns. We're particularly pleased to see the inclusion of compliance agreements and an extended appeal period, as those take some important initial steps towards resolving long-standing problems with PIPEDA's complaint mechanism. We hope that additional changes will be considered at the next statutory review of the bill, which is coming up in the next couple of years. We particularly point to long-standing problems with the lack of proactive compliance incentives as something that we think still needs to be addressed.

With respect to Bill S-4, I'd like to address three parts of the bill very briefly: the new consent requirement, breach notification regime, and some of the information sharing exceptions.

Clause 5 of Bill S-4 will enact proposed section 6.1 of PIPEDA, which seeks to strengthen the consent obligations so that individuals will be aware of the nature, purpose, and consequences of the activities that an organization seeks to carry out with their data. In general, this will mean that where an organization targets or becomes aware that it's dealing with vulnerable individuals such as youths, additional steps to ensure that its privacy practices are understood will have to be taken.

If dealing with young children, it may not be possible at all to make the young children themselves aware of the consequences of their actions, and verifiable parental consent might be required. This is in line with industry practices for minor-specific sites that interact with very young children. There are already legal obligations in some jurisdictions, such as in the United States, under COPPA.

The consent provision will also have a positive impact in other contexts. Strengthening the obligation of organizations to ensure that customers are aware of the nature and consequences of data practices will help individuals make more informed privacy choices in general.

We're a little concerned that recent changes to the bill over its predecessor may shift the focus of the provision to individuals whom the activities are directed at, as opposed to specific individuals whom the organization is dealing with. We're concerned in particular that one common practice would, for example, put in a privacy policy that no children under 13 are permitted on the service; then, when they become aware that large numbers of children under 13 are using the service, the way the consent is phrased might be taken to preclude the additional obligations that should normally apply in that context.

With respect to Bill S-4's breach notification obligation, we're very grateful to see this notification obligation coming into force. It's much delayed and needed. The breach notification obligations have become a standard for 47 states throughout the U.S., and the White House recently announced a federal breach notification bill.

● (1140)

The breach notification regime that Bill S-4 would enact requires that individuals and the Privacy Commissioner be notified where a breach of security safeguards creates a real risk of significant harm. As are my colleagues from the Canadian Bar Association, we're concerned that the standard for notifying the Privacy Commissioner is too high. Additionally our experience has been that it's very useful to have notification directly to the Privacy Commissioner of a majority of breaches for tracking purposes and to generally improve incentives to adopt rigorous technical safeguards.

Even a breach of safeguards that does not lead to the risk of significant harm can be indicative of a general laxity in technical safeguards that should be addressed. We think it's good to have a notification requirement to the Privacy Commissioner that's more comprehensive even where there's no real risk of significant harm to specific individuals.

We're very grateful to see a penalty regime for instances where the breach notification obligations are knowingly ignored. We think that at least over time it would be good to improve this into a more generalized administrative monetary penalty regime. The fines currently in PIPEDA are designed as penalties for very overt offences. An administered monetary penalty regime would be more fitting as it would be focused on securing compliance. That gives businesses more leeway where innocent mistakes are made on the one hand and it may have more teeth where repeat offences are made or where there's a need to secure compliance. I think that would help improve the rigour of this bill, this breach notification regime.

I'll speak briefly to the information sharing elements of the bill. We find a number of these problematic. They raise some potential issues particularly on the private sector side, but we also have some concerns on the public sector side as well. Subclause 6(10) of Bill S-4 replaces the current investigative bodies exception, which permits an exhaustive list of non-governmental regulatory bodies such as the Law Society of Upper Canada to receive information relating to an investigation.

The issue that's intended to be addressed is the difficulties inherent in getting listed as an investigative body. New bodies emerge on occasion, the names of existing bodies change, and each time this happens regulations need to be passed. It's an onerous process. We support addressing that issue.

We're a little concerned that the remedy adopted to address that exception may open the door to unwanted information sharing, particularly in the context of intended lawsuits or where a private company wants to investigate the customer of another company. The provisions adopted in Bill S-4 are an improvement over those in Bill C-12 because they limit the situations in which a company can disclose their customers' information to another company to situations where it can reasonably be expected that if the customer were aware it would compromise the investigation or the impending lawsuit.

● (1145)

However, we're still concerned that this will open the door to customer sharing in a context where the courts have said very specifically that there's a specific process for when you're looking to go after an individual with a potential lawsuit. What you should be doing is filing a statement of claim and going through third party discovery processes, which have built-in safeguards for privacy.

We're concerned that this exception will at the very least give some companies the impression that they will be able to disclose their customers' information. We've had some fairly prominent examples of this in Canada. Some ISPs have been asked, in court so far...because the Federal Court of Appeal has said to date that you cannot disclose your company's information to a potential plaintiff without a court order.

Some of these have gone through the court system and they have even been problematic there. Copyright trolls have asked for the identities of thousands of ISP customers. We've seen other examples where this type of thing could be problematic, so we would appreciate clarification that this exception is not intended to facilitate the types of requests that are to facilitate lawsuits in essence.

We also have some brief concerns relating to proposed section 10.2, which is part of the breach notification regime, which obligates companies who are already disclosing to an individual and to the Privacy Commissioner that a breach of security safeguards has occurred. These companies will also be obligated to notify an open-ended list of companies and government bodies that they believe might assist in the reduction of harm.

In principle, this exception is logical. However, we would like to see some more safeguards in this exception.

Part of the issue is that many agencies that deal with security, particularly in the cyber context, are the same agencies that also conduct investigations on a range of other issues, and security can implicate the private data of several thousand if not tens of thousands of individuals. We're concerned that more information than is necessary may get passed along in these exchanges when they occur.

**The Chair:** Mr. Lawford.

**Mr. John Lawford (Executive Director and General Counsel, Public Interest Advocacy Centre):** Thank you very much, Mr. Chair.

Honourable members, my name is John Lawford. I'm the executive director and general counsel of the Public Interest Advocacy Centre, a national non-profit, federally incorporated organization founded in 1976 that provides legal and research services on behalf of consumer interests, and in particular, vulnerable consumer interests.

Due to the time I'm going to be speaking today solely to the breach notification amendments. However, I'll be happy to take questions on other aspects of the bill.

PIAC believes that the goal of an effective data breach notification law is to actually notify individuals of the loss, unauthorized access, or theft of their personal information from an organization whenever it is possible for the individual to take steps to avoid financial, reputational, or other harms, or to minimize these impacts. In our view this goal can be accomplished in a manner that also removes conflicts of interest in reporting breaches; reduces compliance cost and risk for business, in particular small business; generates data for better policy outcomes; engages, improves, and leverages the expertise of the Office of the Privacy Commissioner, OPC, in dealing with breaches; and encourages business and consumers to make investments in data security.

Unfortunately, Bill S-4, as written, will very likely result in fewer reported breaches than even now and operate in an opposite manner. Namely, it will create a culture of fear, recrimination, and non-reporting. Bill S-4, incentivizes not reporting data breaches by leaving the determination of whether a breach creates a real risk of significant harm to an individual totally in the hands of the organization that suffers the breach. This obvious conflict of interest is fatal to the purpose of the bill as there is no advantage to a company to report and every advantage to hide a data breach.

The conflict of interest in having a company assess whether an individual faces a real risk of significant harm from a data breach is one that will be settled in close cases and some more egregious ones by the company concluding there is no such risk. Such an assessment avoids the cost, reputational damage, and inconvenience faced by the company. It also avoids putting the company on the radar of the OPC for an audit or an investigation.

While it's true the company does face prosecution under the amended section 28 of PIPEDA and a possible fine up to $100,000, perhaps even per record, that offence is premised on not reporting a breach knowingly. Any organization that sets up even the most basic process to come to a conclusion that a breach was not a real risk of significant harm would have a very strong defence. This flaw is exacerbated by the bill's requirement to report all breaches regarding a real risk of significant harm simultaneously and relatively instantly to the OPC, whose role is purely observational, to affected individuals and to unspecified third parties who may be able to help. Which individuals to notify will be determined solely by the company involved, which will be dealing with the chaos of several reporting requirements that frankly make little sense as structured. The incentive again will be to keep the reporting to individuals to as few in number as possible. Contrast this with our vision of how Bill S-4 could work.

Step one, replace the initial reporting to all parties on the real risk of serious harm test for the requirement to immediately report material security breaches involving personal information to the OPC only. In Bill C-12 of the previous parliament, in that version, proposed section 10.1, did this very well with one exception. We would recommend removal of the systemic problem assessment, which the bill required and which also led to the disincenting of reporting.

Step two, leave the decision of whether to order—and yes, I said order—a company to report a data breach to individuals to the OPC. The company would have no say in the matter. The OPC would be an impartial third party arbiter of whether a breach was a real risk of significant harm to affected individuals. The OPC would gain experience, expertise, and authority in assessing breaches. The OPC decisions would be made public, meaning Canadians would finally know which companies had breaches, because this is presently not known for all breaches under the voluntary breach notifications referred to and the private conversations that we know the Office of the Privacy Commissioner has with companies.

Finally, the gathering of security failings generates data that could lead to better policy outcomes based on encouraging companies to invest in improved data security.

● (1150)

This approach would also benefit business, especially small business. With the OPC making the individual notification call, the business would be relieved of the compliance costs in hiring consultants to manage its data breach response, as the OPC would specify when, how, and how much notification was required. It would virtually eliminate the risk of civil liability for data breaches. The OPC could provide extensive breach notification guidance and materials to ease the reporting process for business in dealing with the stress of a breach.

This committee could save time and effort in designing step two by essentially copying the relevant section of Alberta's Personal Information Protection Act, namely section 37.1 of that act.

Finally, a rewrite of Bill S-4, as suggested, should encourage both business and consumers to take personal information security and the response to it more seriously. For business, a step-one requirement to report security breaches to the OPC would drive investments to improve systems in order to avoid having to report breaches. For consumers, a step-two notification could be treated as authoritative, serious, and OPC-approved assurance of impartiality, and spur consumers to take action to appropriately deal with breach notification and, finally, to reflect their judgment of the information-handling practices of the business to those businesses.

Thank you very much. I await your questions.

● (1155)

**The Chair:** Thank you, Mr. Lawford.

I have one brief here, but anything else that the witnesses want to submit in writing to the clerk, particularly because of the situation we're in right now, will be handled as regular evidence.

Colleagues, my job is to be as fair as possible, and we do know that the vote will be approximately at 12:02, so I have the choice of adjourning right now for fairness, or the best math I have in my head is six, four and a half, and three minutes. That's the quick math that I think would be representative of the percentage of people. It would eat into after the bells went on by about seven or eight minutes. I need to have unanimous consent in that regard if we're going to move ahead like that.

**Some hon. members:** Agreed.

**The Chair:** Great, okay. It will be six, four and a half, and three minutes.

Go ahead and begin, Mr. Lake.

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

Sometimes it can be a little bit of a strange place in terms of scheduling, so we'll do the best we can with what we have.

Mr. Lawford, I am interested to hear your points because yesterday, at the last meeting, the witnesses who came before us talked a lot about how even the notion that organizations would have to track breaches within their own organizations was too onerous. In fact, I think that was even brought up today. You seem to be going a step further and saying that virtually all breaches would need to be reported to the Office of the Privacy Commissioner, which seems to be very much on the other end of the spectrum in terms of approaches to this. Maybe that means that we've struck a good balance here.

**Mr. John Lawford:** I would disagree. I think that Bill C-12 which was previously there, had made the effort to set a bar for material breach reporting to OPC, which was based on the seriousness of the information lost and the number of people affected. Again, it also threw in this business about systemic problems, which I think is complicating things. That would mean that the number of material breaches reported to the Privacy Commissioner would not be overwhelmingly burdensome because it would be larger breaches affecting people in a serious way.

**Hon. Mike Lake:** Mr. Israel, in your comments you seem to agree with the Canadian Bar Association—I made a note here—that the threshold for breach notification to the Office of the Privacy Commissioner was too high. Was that what you were saying? I wrote the note down a little bit after you'd said it. I got the sense from the Canadian Bar Association that it might be saying something a little bit different from that, and not actually be on the same page as you at all.

Maybe I'll go to Ms. Morin and get some comment on that. Are you on the same page in terms of what Mr. Israel said?

**Ms. Suzanne Morin:** No, you're right. When Mr. Israel referred to the different thresholds, I think the only thing that we're agreeing on is that there should be two thresholds, but not that more should be reported to the OPC.

**Hon. Mike Lake:** Okay. Mr. Israel, just to make sure that we're on the same page, what you meant to say was....

**Mr. Tamir Israel:** Sorry, I agree that there should be two thresholds, but the second threshold should be an OPC reporting threshold. What I was trying to say was that, as my colleague mentioned, businesses have a clear understanding of what the two thresholds are for. One is for tracking the types of breaches that occur, and one is for ensuring that individuals are able to redress any potential harm that might come to them from the disclosure.

For us, the tracking must happen at the Privacy Commissioner level if we are to have a global and systemic understanding of the types of breaches that are happening, and if we are going to start addressing these breaches at a systemic level and start improving the technical safeguards in all our services, which is where we really need to go. That's the only way to solve breaches in general, so that's what I meant.

**Hon. Mike Lake:** Because our time is so tight here, I'm just going to go to all three of you, in a sense, and ask this question. Are we better off with Bill S-4 as is, than prior to Bill S-4, than we are currently, in a sense? If we pass Bill S-4 as it is, are we better off with our privacy legislation than we were before?

● (1200)

**Mr. John Lawford:** I would like to say that if this bill didn't pass it wouldn't be the end of the world because the breach notification guidelines that are voluntary now are producing. I think you will probably end up with more breach notifications than you would after this bill. That's our view.

**The Chair:** Mr. Israel.

**Mr. Tamir Israel:** We would like to see it go through with some minor amendments.

**The Chair:** Ms. Morin.

**Ms. Suzanne Morin:** Actually, in a way I would echo Mr. Lawford. In particular, as regards breaches, there has been extensive voluntary compliance because industry does actually see their security safeguard obligations requiring notification to individuals. Maybe the only little piece that Bill S-4 brings is the reporting to the OPC, but that's actually happening on a voluntary basis because of the excellent guidelines that the OPC has issued.

**Hon. Mike Lake:** I'm going to come back to you, Ms. Morin, on your first point. You made a couple of key points, recommendations. Your first point dealt with this investigative bodies change. When we were talking about this in our previous meeting, I asked the question of the Privacy Commissioner whether the proposed system is similar to the Alberta and B.C. systems, to which he said it is, absolutely. We have a clear history, a clear precedent, in looking at the Alberta and B.C. systems that says those systems have worked and there have not been significant problems with them.

Can you give me an example of something you're worried about that hasn't actually happened within the Alberta and B.C. contexts, and why?

**Ms. Suzanne Morin:** From the CBA's perspective, we totally understand the movement from investigative bodies to the regime that's proposed in Bill S-4, which is similar to B.C. and Alberta, as you just stated. Because of the concern we had been hearing in the media and others, when you read the words on the page, we thought that maybe there's an opportunity just to rein it in a little bit, so we proposed very targeted amendments to more reflect what actually happens in practice today under investigative bodies. It was more in keeping with the environment of the time, I think, that those recommendations are being proposed.

**The Chair:** Thank you very much, Mr. Lake.

[*Translation*]

Ms. Borg, you have the floor for four and a half minutes.

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

I will keep my questions short so that there is as much time as possible for the answers. I have two questions.

My first question is for all the witnesses. Since this bill was drafted, we have had the Spencer decision.

Do you think the committee should introduce amendments or make some changes as a result of that decision?

[*English*]

**Mr. Tamir Israel:** Ideally, proposed paragraph 7(3)(c.1), which was at issue in Spencer, was one of the more controversial paragraphs that were dealt with in the consultation that led to this bill. Our position then, as it is now, is that it should be struck. We think that Spencer understates that.

Spencer closes the door to some sharing in specific contexts, but there are still ambiguities around what's going to happen in other contexts, and in the interim when that exception was introduced, literally millions of Canadians' private information was given to law enforcement under criteria we're not comfortable with. We would like to see it shut down, and have that provision repealed.

We'd also like to see the inclusion of an individual notice obligation whenever a private company voluntarily provides information to the state, unless it impacts on an investigation or something to that effect. We would like to see that.

Those are things we have, for a while, been calling for and that we would like to see in PIPEDA sooner rather than later.

**Mr. John Lawford:** From PIAC's point of view, the amendment to remove or change the information sharing between corporations needs to be looked at because, as Tamir mentioned, there is some risk of companies using that in contexts like copyright against consumers, where judicial process would give them more protection and is far more appropriate. I see no safeguards and I anticipate there would be some misuse of this section. For that reason we would recommend some amendment in that section.

● (1205)

[*Translation*]

**Ms. Charmaine Borg:** Thank you.

Ms. Morin, what do you think about that?

**Mr. Suzanne Morin:** Clearly, our position is different. We don't think amendments need to be proposed for PIPEDA or Bill S-4. The Supreme Court did its homework, which was to interpret one provision in an existing piece of legislation. We therefore don't think amendments need to be made.

**Ms. Charmaine Borg:** Thank you.

My second question is for Mr. Israel and Mr. Lawford.

In terms of the compliance agreements, we know that one of the objectives of the bill is to ensure that organizations are really taking PIPEDA seriously, which is unfortunately not always the case right now.

Do you think the compliance agreements proposed in Bill S-4 are sufficient to really encourage organizations to comply with Canadian law?

[*English*]

**Mr. Tamir Israel:** The addition of compliance agreements is helpful, but it addresses a very specific scenario. What happens with a privacy complaint is that it goes to the commissioner, she does her report, and she issues a recommendation. It's a non-binding recommendation, so let's say the company agrees to comply. If it changes its mind a year later, you basically have to start from scratch and file another complaint. There is no mechanism to make that enforceable.

The compliance agreements help a lot in that context, but they don't help with one issue that we're concerned with, which is to put in place incentives for proactive compliance. For that to be in place, you need some type of potential damages to happen if you violate the principles of PIPEDA in a very clear and egregious way. We think that's needed for PIPEDA. Most other privacy and data protection commissioners around the world have those types of powers. We would like to see that in PIPEDA as well.

Thank you.

**Mr. John Lawford:** I generally agree with Mr. Israel. Compliance agreements are a kind of band-aid. What you're really looking for, I think, is order-making power on behalf of the commissioner. It will help with some situations. However, long negotiations with companies may or may not actually have the result that the Privacy Commissioner wants, even with compliance agreements.

**The Chair:** Thank you.

We'll now go to Ms. Sgro for three minutes.

**Hon. Judy Sgro (York West, Lib.):** Thank you very much, Mr. Chair.

Mr. Lawford, you're not happy with where Bill S-4 is.

**Mr. John Lawford:** No.

**Hon. Judy Sgro:** It's very clear that you think there's just too much: it has to be a material breach, it's this, it's that; it's not clear enough.

How could we clarify it and make it stronger, so that it would satisfy you and your organization?

**Mr. John Lawford:** We are proposing today a hybrid model, one that looks a lot like what was in Bill C-12. In order for it to be two steps, you would have to have a reporting of material breaches of security safeguards, as it was worded in that bill, that affect personal information, as a first step, only to the Privacy Commissioner. Then, as in Alberta, it's better to leave the decision about whether to notify individuals with an impartial third party, the Privacy Commissioner, rather than again leaving it up to the company, which is what this bill.... It places a lot of responsibility on companies, actually. If they make a call badly, it's just preferable to leave it in the hands of an impartial third party.

That would be what we propose, that two-step approach.

**Hon. Judy Sgro:** On the issue of risk, the company can probably argue that they didn't think it was of significant risk so they didn't report it. They can appeal and get around the system that we're trying to put in place.

**Mr. John Lawford:** That's our concern, that the assessment done by the company may not be taking factors into account that the Privacy Commissioner might think of. They have a limited view; the Privacy Commissioner will have seen lots more situations.

It's not malicious. It's just what will happen.

**Hon. Judy Sgro:** It's just the way it is.

**Mr. John Lawford:** Yes.

**Hon. Judy Sgro:** Ms. Morin, you mentioned the concern about the record-keeping, or your colleague did, and that it would be very difficult to keep track of it all, and so on. Do you want to elaborate a bit further on that issue?

**Ms. Suzanne Morin:** I did hear the testimony earlier this week where that came up. Maybe I can give you a really quick example of it.

Take a call centre context, where someone calls in and says, “I received the bill of my neighbour at my home.” What would happen in that context is that the call centre representative would say, “Oh, that's horrible. We'll send you an envelope; can you please send the bill back to us?” Then the call centre representative would reach out to the other customer and say, “We're very sorry, but your neighbour received your bill. We apologize.” They would then make amends.

That situation is technically a breach of security safeguards, because the wrong bill went to the wrong customer. It's a one-off. It's not insignificant to those two customers, but it's insignificant in the grand scheme of when you think about breach notifications. The way Bill S-4 is worded today, it would require us—by “us” I mean any industry or organization subject to PIPEDA—to develop a system to log that somehow. It's taken care of. It's managed. It's handled. But it would have to be logged somehow, through a different system. Otherwise the organization is subject to new offence provisions, which are very serious. The breach notification offences are quite serious in the record-keeping—

● (1210)

**Hon. Judy Sgro:** But doesn't that go back to the company having sloppy processes in place? That's just one example. I suspect there are probably lots of examples.

**The Chair:** Very briefly....

**Ms. Suzanne Morin:** Every organization has breaches of their security safeguards. That goes without saying. Some are more significant to Canadians, broadly speaking. Others are not. We should focus on those that are of the most concern to Canadians.

**The Chair:** Thank you very much.

Again, my apologies to the witnesses.... Thank you very much for your indulgence in our democracy. I appreciate it. If there's anything else that you'd like to submit, please do so in writing and we will treat that as evidence.

Colleagues, if you would indulge me for one more minute, there's an item that we have to deal with in camera that normally only takes 60 seconds. I can suspend for a couple of minutes. We have quite a window of time since it's down the hall.

Let's suspend for a couple of minutes to clear the room.

[*Proceedings continue in camera*]