HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Industry, Science and Technology

INDU • NUMBER 037 • 2nd SESSION • 41st PARLIAMENT

EVIDENCE

Thursday, March 12, 2015

Chair

Mr. David Sweet

Standing Committee on Industry, Science and Technology

Thursday, March 12, 2015

● (1140)

[*English*]

The Chair (Mr. David Sweet (Ancaster—Dundas—Flamborough—Westdale, CPC)): Colleagues, ladies and gentlemen, *bonjour, mesdames et messieurs*.

We are in the 37th meeting of the Standing Committee on Industry, Science and Technology.

I'm going to introduce our guests very quickly, but I want to give a heads up to all the members at the table. Maybe there could be some conversation among the parties offline and we could begin the clause-by-clause examination on March 31. We have no other witnesses at that point. For many reasons, many of the witnesses who were put forward by all parties decided not to testify before the committee. With that in mind, we can move up the date a little bit on clause-by-clause study, if everybody is ready.

I'll leave that to some informal conversations, and then you can advise the clerk or me as to your readiness for that eventuality.

Before us today is the British Columbia Civil Liberties Association, Micheal Vonn, policy director.

From the Canadian Bankers Association—

Was it the Canadian Bankers Association that was stuck on the tarmac the other day? No, it was the insurance...? Sorry. I was simply going to offer our deep regrets that you had to suffer in a plane and then had to come here, but I'll save that for the appropriate folks.

—we have Linda Routledge, who is director of consumer affairs, and William Crate, director of security and intelligence.

From OpenMedia.ca we have Meghan Sali, campaigns coordinator.

From the Retail Council of Canada we have Jason McLinton, senior director of federal government relations, and Karl Littler, vice-president for public affairs.

I have a problem here on my orders of the day. That won't happen again.

Mr. John Carmichael (Don Valley West, CPC): It's a tough day.

The Chair: I know; it's really tough.

We'll follow the orders that are before us and will begin with Ms. Vonn's opening remarks.

Ms. Micheal Vonn (Policy Director, British Columbia Civil Liberties Association): Thank you, Mr. Chair.

Again, my name is Micheal Vonn. I'm the policy director of the British Columbia Civil Liberties Association. We are of course a non-partisan, non-profit society and one of the oldest and most active civil liberties and human rights organizations in the country. Privacy is a key portfolio of our association, so we are very grateful to be asked to speak to you today on Bill S-4 and particularly pleased that we are able to discuss it with you prior to second reading, while the scope of the bill is still open for discussion.

Our association would like to support and echo many of the concerns and recommendations that have already been brought before this committee by civil society and academic witnesses. For example, we strongly support the position of B.C. FIPA that there is an urgent need to bring federal political parties under PIPEDA.

We also endorse the position of the national PIAC that compliance agreements are of limited assistance in protecting Canadians' privacy rights and that it is long overdue for the federal Privacy Commissioner to have order-making powers, like provincial counterparts. We believe lt is unacceptable that statutory privacy rights that courts characterize as quasi-constitutional are regulated federally largely on the basis of moral suasion without effective enforcement. ln our view, Bill S-4 falls far short of addressing this critical and long-standing problem.

However, time being limited, I will devote my prepared remarks primarily to the Supreme Court of Canada's decision in R. v. Spencer and its implications for Bill S-4.

The Spencer decision, as you know well, dealt with the provisions of PIPEDA that allow for disclosure without consent to government institutions when the institution has identified its lawful authority to obtain the information. The issue in the case was whether the police seeking access to subscriber information without a warrant from an Internet service provider had the requisite authority. The answer to that question depends on whether there is a reasonable expectation of privacy in customers' subscriber information.

The Supreme Court of Canada resolved this issue, on which lower courts had been divided, and found that there is a reasonable expectation of privacy in subscriber information and that it is reasonable for Internet service users to expect that a simple request by police would not trigger an obligation to disclose information or defeat PIPEDA's general prohibition on the disclosure of personal information without consent.

For the purposes of our section 8 charter right to be secure against unreasonable search and seizure, a request by a police officer that an Internet service provider voluntarily disclose subscriber information amounts to a search, and a warrantless search is presumptively unreasonable, according to section 8 analysis that you will find in R. v. Collins. The crown bears the burden of rebutting this presumption by showing three things: one, that the search is authorized by law; two, that the law itself is reasonable; and three, that the search is carried out in a reasonable manner.

Now, the question in Spencer was whether or not the provision in PIPEDA ostensibly allowing for disclosures without consent to law authorities was in fact a law authorizing this. The court said it was not. If it were, the court said, in paragraph 70: ...

> PIPEDA's protections become virtually meaningless in the face of a police request for personal information....

The court said that of course the police have lawful authority to ask questions relating to matters that are not subject to a reasonable expectation of privacy and of course they have lawful authority to conduct warrantless searches where there are exigent circumstances. But “lawful authority”—that language in PIPEDA as it stands—requires more than a bare request. This we know from Spencer.

Thus we say that there is a need in Bill S-4 to amend the provision that is at issue in Spencer, a provision so confusing that we had to go all the way to the Supreme Court of Canada to have it definitively interpreted. And while some very limited and narrow voluntary disclosures may still be viable under this provision post-Spencer, outside of exigent circumstances such disclosures would require legal advice.

● (1145)

lt is patently unreasonable to maintain a provision that cannot be understood on its face and requires a charter analysis to be used appropriately. As we argued in our lawful access report of 2012, the best approach is to remove this provision in its entirety.

Alternatively, we say that the term “lawful authority” could be replaced by the term “statutory authority” for greater clarity, however the constitutionality of said statutory authority will, of course, ultimately still be a question of debate.

The further question of the constitutionality of express statutory authorities for disclosure, in light of the Supreme Court of Canada's decision in Spencer, has led the special committee reviewing PIPA in British Columbia to call for a narrowing of its voluntary disclosure provisions under the act.

We want to caution this committee that there are at least two reasons we cannot look to Alberta and British Columbia's privacy legislation relating to the private sector for assurance that proposed expansions of voluntary disclosures found in Bill S-4 are likely to go well.

One, there is a clear concern that those PIPA provisions may not be constitutional in light of Spencer.

Two, however little historical challenge there has been in relation to those provisions thus far, the same will certainly not be the case in relation to the arenas governed by PIPEDA, which obviously include telecommunications.

I have other things that I could say about this, but I think I'll save it for questions.

Thank you very much.

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

We'll now move to the Canadian Bankers Association.

Please go ahead with your opening remarks.

Ms. Linda Routledge (Director, Consumer Affairs, Canadian Bankers Association): Thank you, Mr. Chair, and thank you for having us here today.

The banking industry has long been a leader in privacy protection. Given the nature of the services that banks provide to millions of customers in communities across Canada, banks are trusted custodians of significant amounts of personal information. Privacy and protection of clients' information is a cornerstone of banking. Banks take very seriously their responsibility to protect customers' information and are committed to meeting not only the requirements of privacy laws, but also the expectations of our customers.

We are pleased to have this opportunity to voice our support for the many provisions in this legislation, including the new breach notification and the financial abuse provisions. We are concerned that amendments to eliminate investigative bodies will create uncertainty and may significantly limit the type of information that banks currently share to prevent criminal and terrorist activity.

The banking industry supports the requirements in the digital privacy act for organizations to notify individuals about a breach of their personal information where there is a risk of significant harm. ln fact banks already notify clients in the rare instances of such a breach so that individuals can protect themselves from fraud or any other misuse of their personal information. We are in favour of reporting material breaches to the Privacy Commissioner. We also support the commissioner's new oversight powers to ensure that organizations comply with these new provisions.

We look forward to working with the government on guidance and regulations to set out the details of how these provisions will be implemented, thereby providing an effective framework to ensure that Canadians are notified in a timely manner. lt is important for all stakeholders to work together to protect the personal information of individual Canadians, and Bill S-4 effectively creates a framework for this to happen.

The CBA has long advocated for amendments that will help seniors and vulnerable Canadians from becoming victims of financial abuse. We applaud the government for including an important amendment in Bill S-4 that would allow banks to notify a family member or authorized representative in suspected cases of financial abuse. When bank employees see situations in the branch that suggest potential financial abuse, it is the customer's savings that are at risk, and bank staff want to be able to help them to avoid financial abuse.

At present PIPEDA only allows a bank to report suspected cases of financial abuse to a government institution, such as the police or the public guardian and trustee, and only where there are reasonable grounds to believe that a law has been contravened. The suspicious behaviour that bank staff may witness may not necessarily suggest that a law has been broken. lt can still be a case of financial abuse and yet banks are constrained in what they can do to help their clients. Even when banks suspect unlawful behaviour, and are able to report the suspected abuse, they are often told that police or the public guardian and trustee do not have sufficient resources, or sometimes even the mandate, to undertake an investigation on financial abuse.

Our support for this provision is guided by the best interest of our customers, particularly groups most susceptible to financial abuse such as seniors. Banks want to ensure that their staff have the ability to protect their customers from financial abuse, and this provision is an important tool in this regard.

While we are supportive of the majority of the provisions in Bill S-4, we are concerned that some of the proposed amendments may hinder the ability of banks to protect our customers, our employees, our communities, and the financial sector from crime.

Current regulations under PIPEDA contain a list of designated investigative bodies through which organizations can share personal information under conditions set out in the act. The CBA's bank crime prevention and investigation office, or BCPIO, was among the first investigative bodies approved by the government, and it has been in operation for almost 15 years. The BCPIO's information-sharing policies and procedures across organizational boundaries are clearly understood by Canadian banks, along with other participating financial institutions. lt is this formal relationship that allows banks to detect, prevent, and suppress criminal activity such as theft of data and personal information, criminal breach of trust, proceeds of crime, money laundering, terrorist financing, cybercrime, bank robberies, and physical attacks on critical infrastructure.

● (1150)

The bill proposes to replace designated investigative bodies with a framework for the disclosing and sharing of personal information among organizations. ln our view, the new provisions, particularly the wording of proposed provision 7.(3)(d.2), may not allow banks the same scope as the investigative bodies to detect, prevent, and suppress the full range of criminal activities. ln particular, we are concerned that the proposed change limits disclosure to circumstances where it is "reasonable for the purposes of detecting or suppressing fraud or of preventing fraud". Many of the criminal activities I listed earlier are just not captured by the term "fraud".

If these provisions are passed in their current form, we believe the ability of the banks to protect the financial system and our customers from criminal activity may be severely hampered.

We ask the committee to consider amending the bill to allow approved investigative bodies such as the BCPIO to continue with their important work. Alternatively, if the committee wishes to maintain the proposed approach in Bill S-4, we recommend that the legislation be amended to ensure financial institutions can share the information needed to detect and prevent other types of serious criminal activity beyond fraud.

ln closing, we want to reiterate the banking industry's support for many aspects of Bill S-4 and ask the committee to consider amending the bill to help protect Canadians from financial crimes.

We would be pleased to answer your questions.

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

Now on to Ms. Sali for your opening remarks.

Ms. Meghan Sali (Campaigns Coordinator, OpenMedia.ca): Thank you, Mr. Chairman.

Good afternoon, my name is Meghan Sali. I'm here today on behalf of OpenMedia, a non-profit organization working to safeguard the digital rights of Canadians. I'll structure my remarks today by focusing primarily on a critical issue within Bill S-4, which, if passed in its current form, could expose Canadians to an unwarranted exploitation of their private data.

Subclause 6(10) proposes to expand voluntary disclosure of sensitive information by a private company, most notably in our estimation, by telecom providers. It would also allow for involved service providers to offer this information to anyone without the consent of the individual.

Today I will briefly cover a few points central to this issue, including the sensitivity of basic subscriber information, the overly broad disclosure framework in Bill S-4, and the lack of trust concerning the entities seeking disclosure.

Flagging a common use case for such provisions, I would ask you to imagine a private company seeking to sue the customers of Internet service providers based on the anonymous online activities they see. Before they can proceed, this company would like the ISP to identify who is behind the IP address, by voluntarily turning over basic subscriber information. Considering that a report issued by the Privacy Commissioner just last year outlines how online identifiers can be extremely revealing, potentially conveying information about a person's medical status, religious views, sexual orientation, political affiliation, and more, the argument against this information being considered “basic” is extremely compelling.

As you know, Bill S-4 also comes on the heels of a Supreme Court of Canada ruling that Canadians have a reasonable expectation of privacy with regard to this type of information. In the Spencer ruling, with regard to IP addresses, the Supreme Court stated:

> The user cannot fully control or even necessarily be aware of who may observe a pattern of online activity, but by remaining anonymous — by guarding the link between the information and the identity of the person to whom it relates — the user can in large measure be assured that the activity remains private...

Or as a supporter, Shawn, wrote on our website:

> We have a right to privacy, and to not be subjected to criticism or surveillance based on meta data.

Additionally, a number of courts have spoken out about the need for privacy protections to prevent abuse by private companies trying to sue the customers of ISPs. As with previous presentations, OpenMedia invited citizens to share their concerns concerning Bill S-4, and to help shape my testimony today. I think it's important for MPs to put the lived experience of Canadians front and centre in these deliberations.

Dave Carter had this to say in a comment submitted on our website:

> No company, public or private should have a right to access my personal, private information without following due course of procedure through obtaining a court approved warrant. This is akin to a stranger cutting the keys to your house and letting themselves in whenever they want to snoop through your socks and underwear drawers.

I will now move on to my second point. The framework under Bill S-4 allows disclosures for the purpose of investigating the breach of an agreement, or a contravention of the laws of Canada or a province, that has been, is being, or is about to be committed. Experts and the Privacy Commissioner have indicated this framework is overly broad, and that allowing the voluntary disclosure of personal information, simply on the basis of an investigation, could lead to a violation of privacy rights. Disturbingly, the scope of such private investigations is not defined in this bill.

As supporter K.A. told us on our website:

> A law letting a private company share individuals' private information on the mere suspicion of wrongdoing is just too broad a power to have. This is putting a private company, even one with a vested interest in certain outcomes...to become an accuser, judge and jury, for unsuspecting individuals.

This brings me to my final point, which centres on the issue of trust. As I've mentioned, if we were to disclose data that is highly sensitive based on a very loose framework, with no oversight, accountability, or citizen consent, I would expect we would generally have a great deal of trust in the ethics of the entities involved. This bill comes at a time when our copyright notice and notice rules, just implemented in January, are being exploited and distorted. Specifically, media entities and their firms have been sending misleading, and in some cases flagrantly abusive, copyright infringement notices to Canadians. Many of these notices threatened massive lawsuits of up to $150,000, demanded settlements from individuals before any court proceedings, and even threatened users with being kicked offline for unproven accusations of infringement. Some of the notices even mentioned online activity that the user had never engaged in, let alone acquired related files.

One supporter, who asked to remain anonymous, told us in an email:

> I...have received two copyright infringement notices from IP-Echelon which... have accused me of downloading HBO's "Girls", a show I have definitely never heard of.

Another supporter, coincidentally accused of downloading the very same HBO show, forwarded us his reply to TELUS, his ISP. He says:

> I do not know of this show and have no record of downloading or streaming such a show. As the letter is threatening in content and provides no proof of the claims it makes, I would like it if you would provide me with the proof of such an event taking place.

● (1155)

Since January 2015 OpenMedia has seen more than 11,000 Canadians speak out on this issue through our website alone. Thankfully, rights holders and their firms do not have the personal information associated with the IP address, where the notices are being sent. This critical element of our notice and notice provisions maintains that a private entity must obtain a court order to access the personal information of a subscriber. Bill S-4 would undermine this clearly necessary safeguard and associated oversight with a court of law.

The question before you now is, knowing how some firms have already abused our notice and notice provisions, why would we give them unauthorized access to the sensitive personal information of innocent Canadians? Why leave our privacy rights in their untrustworthy hands?

In conclusion, I would like to say that we applaud the steps taken by this government, in particular on telecom and copyright issues, to ensure that customers are treated fairly and respectfully by companies that provide services to Canadians. However, this positive legacy will be put at risk by allowing subclause 6(10) to stand, as more Canadians are exposed to privacy breaches and potentially harassing demands from companies that have demonstrated they are not deserving of our trust.

Thank you for your time, and I'd be happy to answer questions.

● (1200)

The Chair: Thank you, Ms. Sali.

Now to the Retail Council of Canada.

Mr. Karl Littler (Vice-President, Public Affairs, Retail Council of Canada): Thank you, Mr. Chairman.

I think most members will be familiar with RCC, which has been the voice of retail in Canada since 1963. As a not-for-profit industry association, we represent over 45,000 storefronts on a national basis, of all formats ranging from independent through grocer, online, and mass merchandise merchants.

We appreciate the committee's invitation to appear today. While we're not in as strong a position as my friends here from BCCLA and OpenMedia to comment on the legal intricacies of Bill S-4, we would be pleased to provide some general observations from a retail perspective.

Retailers are generally supportive of the proposed legislation, but do believe that it could be improved upon in some areas, which I and my colleague will address.

Generally speaking, Bill S-4 strikes the right balance between action to protect digital privacy on digital fraud and financial abuse, while recognizing the strengths of PIPEDA and its forward-thinking technologically neutral approach. More specifically, we support the clarification on the exclusion of business contact information, as this was clearly not meant to be captured. This section 4 clarification will better equip businesses to conduct their ongoing operations. We also support the provision for more flexible resolutions to breaches of the act's requirements, notably the provision for voluntary compliance agreements in section 15. We also support the reasonable belief basis for reporting in proposed section 10.1.

Turning to the issue of consent in section 5, we do note that it provides that consent is not valid unless how the information will be used is clearly communicated in a language appropriate to the target audience. We certainly agree with the principle. We understand this is the target of that section, that a vulnerable population such as children should be protected.

We don't take the position that some previous witnesses have that this proposal is superfluous and should be withdrawn. That said, we would encourage the inclusion of a provision for regulation to specify which vulnerable groups are covered. While it may be challenging to do so, a regulation could specify a non-exhaustive list including the obvious examples of minors through to those with cognitive disabilities and those lacking full fluency in the language in which they're being served. Further from that, non-prescriptive guidance from the commissioner's office on appropriate best practices would provide practical guidance for merchants.

With regard to record-keeping, we note that proposed section 10.3 requires that records of breaches be kept in a manner prescribed by regulation. Retailers encourage the inclusion of a materiality test for record-keeping specifically, as it would allow for greater certainty and would tend to limit onerous and less helpful record-keeping, where a breach has occurred technically but without any reasonable prospect of material harm. We're thinking of instances like a computer screen being left unattended or a filing cabinet being left open, where a third party may have passed by. We want to avoid the trivial and ensure that there is some material requirement here for the keeping of records.

We would also suggest including a provision specifying a reasonable length of time for record-keeping, perhaps one year, but we're obviously open in that regard. What we don't want is an obligation to keep records in perpetuity, where they may be diminishing in use from the perspective of the public good and would be onerous for merchants to maintain.

With your indulgence, Mr. Chair, my colleague, Jason McLinton, will make two further observations and conclude on our behalf.

Mr. Jason McLinton (Senior Director, Federal Government Relations, Retail Council of Canada): Retailers note with interest the section that grants the Office of the Privacy Commissioner seemingly unrestricted discretion in releasing any information under its control to the public when deemed to be in the public interest. Retailers would like to see some reasonable limitations around this disclosure clause as, understandably, releasing potentially sensitive business information without parameters risks causing serious and irrefutable reputational harm to businesses.

Our final comments relate to single window reporting and compliance. We note that Alberta has legislated in this area and that other provinces and jurisdictions are considering legislating in this area. We encourage the inclusion of a provision that would ensure single window breach reporting and single window compliance agreements, or any sort of other compliance, as other parties consider legislating in this area. An example might be that the Office of the Privacy Commissioner could be given the ability to waive reporting requirements when suitable notification has already been given in another jurisdiction and handled there. This would avoid unnecessary and potentially administratively onerous double reporting with different formats or multiple compliance requirements.

To conclude our comments, retailers support the bill but think it could be improved by some targeted amendments. We would of course be delighted to work with this committee, Industry Canada, and the Office of the Privacy Commissioner to help secure those improvements.

Thank you.

● (1205)

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

Colleagues, because of votes we're obviously constrained, so we will have five minutes straight across.

Mr. Daniel, please begin.

Mr. Joe Daniel (Don Valley East, CPC): Thank you, Chair.

Thank you, witnesses, for being here.

My first question is to Ms. Sali.

Do you think that Bill S-4's new provisions on valid consent will strengthen the protection of children's online personal information, in fact, anybody's information? A lot of the time the consent that you're actually looking for is so complex that I don't know anybody who has actually read through it all.

Would you like to comment on that?

Ms. Meghan Sali: One of the things that we've noted is that in 2012 there was a study that said that a lot of this consent is being signed in disclosure agreements and terms of service agreements. There was actually a study in 2012 that stated it would take 72 work days for an individual to read all of the terms of service that they sign in a year.

Unfortunately, we don't think that's a reasonable expectation, that people would be able to read and understand, especially children, a lot of these things that they are being asked to comment on. I don't think those provisions go far enough.

Mr. Joe Daniel: Thank you.

Would anybody else like to comment on that?

Ms. Micheal Vonn: [*Inaudible — Editor*] ... useful around that qualification of what you are required to do in terms of consent is that it brings to light for the organizations involved that uses of big data, metadata, the kinds of data analytics that many people don't consider when they are looking at consent simplicitors. They need to be alive in their minds to the modern usage of data and informing people about how they intend to use these new analytical tools. That's one of the advantages we see to this calling of attention to consent.

Mr. Joe Daniel: I think the other thing is, there are many things that are hidden in there such as marketing use of your data, etc., that you're signing off on, which is not necessarily something you want to do.

My next question is to the Retail Council of Canada.

You have stated that support to risk-based approach to data breach notification on individuals.... Would you say that Bill S-4 sets appropriate thresholds for notification for individuals?

Mr. Jason McLinton: With regard to reporting, I think it's entirely appropriate. What I note from the language of the bill is that it states that there is a reasonable expectation for significant harm to the individual. There is some definition of that provided there, but I think it allows for the flexibility required because it will vary on a case-by-case situation. I agree with the wording of the bill.

Mr. Joe Daniel: Are there any comments from any of the other groups?

Mr. Karl Littler: I might add something to what my colleague has said.

We have taken issue—and I realize you're talking about reporting now rather than recording—with the way the reporting requirement is framed and do believe there should be a materiality test there. We could envisage circumstances in which there would be a breach, and the matter could be resolved informally between the retailer in their setting and the customer in place. Although technically there's been a breach, the customer has determined that it doesn't bring risk of significant harm. I'm thinking particularly in the areas that are a bit more subjective, like humiliation, or what have you.

We could imagine a world in which it wouldn't seem necessary, then, to conclude that although we have an informal discussion with the customer, that is something that requires a formal notice both to the individual and to the commission. We can see a space in between, if you like, for informal resolution in situ between the merchant and the individual customer.

● (1210)

Mr. Joe Daniel: Thank you.

Bill S-4 includes new provisions that will assist organizations in preventing and combatting fraud. How will these provisions further assist and facilitate these activities? This is directed to the banking association.

Mr. William Crate (Director, Security and Intelligence, Canadian Bankers Association): Canadian banks today are committed to working together to prevent, detect, and suppress, and also respond to crime as it exists in Canada. We do that under our investigative umbrella called the bank crime prevention and investigation office. That currently provides a secure environment.

Our concern is that the bill that's proposed won't affect the investigation aspect at all. Basically, we're here to flag the notion that especially (d.2) may inhibit the ability for the banking sector to share information for non-fraud cases.

The Chair: Thank you very much, Mr. Crate. I'm sorry that's all the time we have.

Ms. Nash.

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

Thank you to all the witnesses for being here. I think all members of this committee, and I'm sure yourselves as well, share the goal of updating our privacy legislation. We think that's long overdue. We all of course have a stake in making sure that our Internet transactions, our financial transactions are safe and secure.

Ms. Sali, you mention that from your ISP number, you can reveal inadvertently all kinds of financial or medical information. Could you just explain for the layperson, the vast majority of us who use the Internet and who give that consent routinely, what kind of information we could be revealing, and why that is of concern to you?

Ms. Meghan Sali: Absolutely. As I noted in my presentation, metadata can reveal extremely personal information about people that also will echo Ms. Vonn's points that these people often don't know is actually being revealed. That can include, as I said, the histories of websites they visit, so it's like looking at cellphone calls.

The metadata for a cellphone call can tell you who you called and for how long you talked to them. It can't tell you the contents of that person's phone call, but it can tell you how many times that person speaks to them, how many times they visit their bank's website, what their bank's website is, what other websites they visit. It can definitely reveal a pattern of behaviour that tells a lot about a person.

Ms. Peggy Nash: So this is the kind of thing that would reveal if I'm searching for cars on the Internet. Then I get advertisements that pop up that try to market cars to me. Is that the kind of thing it can do?

Ms. Meghan Sali: Absolutely, yes, and definitely in more sensitive cases than that—

Ms. Peggy Nash: Yes, if it was that dangerous.

Ms. Meghan Sali: Yes, in more sensitive cases than perhaps buying a car is the opportunity for people who are seeking medical advice or people who are potentially seeking out sources on political information. These are things that people have a reasonable expectation of privacy to and don't imagine would be revealed by just the comings and goings of their IP address.

One of the other things we're also concerned about with this bill is that it doesn't just limit the information that you can reveal to the IP address. It's actually any personal information that company has stored on you that they think may be reasonable for the purpose of their investigation, so that can literally include your e-mail logs. It can include any information that this company has collected on you, and that's definitely something concerning to us.

Ms. Peggy Nash: Thank you.

Ms. Vonn, you're from B.C., and we've heard testimony that where there are problems, where there are unwarranted breaches, or breaches without consent, the provincial privacy commissioner has order-making power. The federal Privacy Commissioner does not. Do you think having order-making power has improved the legislation in British Columbia, improved the enforcement?

Ms. Micheal Vonn: I think it's critical that the Privacy Commissioner has order-making power. As I say, we have no indication here that we've seen any privacy commissioner with order-making power act anything other than sweetly reasonably. There is a question of will this not be heavy-handed, will organizations that make inadvertent mistakes be somehow characterized as bad players, etc.? This is simply not what we're seeing with privacy commissioners who have order-making powers across the country, who still have the ability to use moral suasion, advising best practice and all of the other range of educative tools that we would like, but nevertheless have something backing them up.

To explain to, in our case, British Columbians that your privacy rights are enforceable, I can tell you Canadians are stunned to find out that their statutory federal privacy rights are essentially incredibly difficult to enforce and require an exorbitant amount of resources to take you to an enforcement place.

● (1215)

Ms. Peggy Nash: Thank you.

We heard that the federal bill S-4 is based on the Alberta and B.C. bills, but it's our understanding that B.C. recently conducted a review of PIPA, its provincial legislation, based on the Spencer decision at the Supreme Court. We heard from Vincent Gogolek at our last meeting from the BC Freedom of Information and Privacy Association. He said that what happened was the scope of PIPA, the B.C. law, was narrowed. Now the minister, Minister Moore, feels that Bill S-4, this current bill, is in compliance with Spencer. You seem to have a different point of view. Can you clarify that?

The Chair: Very briefly, please.

Ms. Micheal Vonn: We have not limited those provisions yet in British Columbia. The privacy commissioner has recommended in light of Spencer that they be limited to disclosures that involve the organization in question, so not third party....

The Chair: Thank you very much for that brief answer.

Mr. Warawa for five minutes.

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

Thank you to the witnesses.

My focus and my questions will be on dealing with privacy issues and moving forward.

As you know, PIPEDA became law in 2000. It came into force over 2001 to 2004 and there is a statutory review on most federal legislation and that statutory review took place, I believe, in 2006 or 2008. My question is going to be focusing on whether we should continue to discuss potential amendments to this or we should move forward and get general consensus on Bill S-4 and move it forward. Or do we not move forward on Bill S-4 and ask the next parliament to deal with this.

As we heard from you, Mr. Chair, you're recommending that we start clause by clause on the 31st, because what we've heard, in submissions and from the witnesses, is that there's general support for Bill S-4, from the public and from the witnesses. There are some suggested amendments but some of these changes can be done by regulation following the amendments and passage of Bill S-4 if it does happen. We have a very short window to pass it in this parliament. If we don't, it will be the next parliament and we've already been at work on this almost a year.

That's going to be the focus of my question. Do we move forward or are you suggesting that we not move forward?

I'm going to first go to the Canadian Bankers Association. You were quite involved in the judicial review. You appeared before the committee to express a general support for PIPEDA and then you made a number of recommended changes that are in Bill S-4. Could you highlight some of those changes that you are happy with that are included in Bill S-4?

Ms. Linda Routledge: Certainly, the financial abuse provision was one of the ones that we were very strongly looking for. We also supported having a breach notification and reporting regime. It's something that the banks have been doing for decades, since PIPEDA came into effect and that's certainly a positive.

There were a couple of others. The legislation wasn't clear that schedule III banks were included and the bill has included that as well. So there are a number of the things that we were in favour of.

Mr. Mark Warawa: You are generally in favour of Bill S-4 moving forward. Is that correct?

Ms. Linda Routledge: If we could get that one amendment to expand the ability of banks to share information for the purposes of preventing, detecting, and suppressing criminal activities, not just fraud....

● (1220)

Mr. Mark Warawa: Would Bill S-4 improve protection for seniors and vulnerable groups?

Ms. Linda Routledge: Yes, it would.

Mr. Mark Warawa: It is very important, Chair, that we identify that.

Mr. Littler, you highlighted the support of your organization, the Retail Council of Canada, and you highlighted that there could be amendments by regulation to identify the vulnerable groups. Is that correct?

Mr. Karl Littler: That's correct. There are a number of specific provisions in this bill that we do support, and I had noted especially the business contact information exemption, which is significant here. We are supportive of the sort of alternative route, if you like, of voluntary compliance agreements. There are other aspects in here. On balance, if the section that is intended, although does not explicitly state that it covers protection of vulnerable persons, is to proceed, we would hope to see some elucidation of that on the regulatory side, but, on balance, we would support Bill S-4 moving forward.

Mr. Mark Warawa: Thank you.

The Chair: Mr. Regan now, for five minutes.

Hon. Geoff Regan (Halifax West, Lib.): Thank you very much, Mr. Chairman.

Thanks to the witnesses for joining us today.

Let me start with Mr. Littler. You talked about the idea of a provision, so that a customer could indicate to one of your members in the retail sector that they were basically waiving their rights on an issue that had arrived, that you would notify them that there had been an issue and they would say it was not a problem. What kind of disclosure do you think there would have to be in that case? What should satisfy us in terms of the idea that the person has been really properly informed of what the dangers conceivably could be? We can't just assume that the business is going to do this or do that for the person.

Mr. Karl Littler: I think it's going to be situational. This is not to be fanciful. If somebody's shoe size was revealed to another customer passing by, that is obviously resolvable in the circumstance.

The kinds of harms that are specified are quite varied, everywhere from humiliation to bodily harm to significant financial harm, so I don't know that there is a single answer. Obviously there is a thin skull plaintiff issue here, but where it is something a reasonable person would say there's a risk of significant harm, I think you're frankly into the full reporting regime with a formal report to the individual and a report to the PCO.

In areas that are perhaps a bit more subjective, then if it's possible to get consent for one thing, I suppose it's possible at the same kind of standard to get somebody to indicate they are comfortable there has not been a problem. Now bear in mind there has then been a breach, if you like, so you would still have to record it so that if the person came back later and said, “Well, actually, upon reflection, I'm not happy about it”, at least there would have been a record created.

We are trying to envisage something of a halfway house. This wouldn't preclude that. There is nothing in here that would preclude some informal resolution because if it didn't hit the reasonable risk of significant harm test, then there can still be notice and informal resolution below that level, and could conceivably be worked out between the customer and the retailer, recorded by the retailer as a matter of course under proposed section 10.3.

You'll also bear in mind there are circumstances that we would envisage where something wouldn't even reach the 10.3 level where it's such a technical breach that it doesn't hit the standard in the other sections. We almost envisage three scenarios, one in which it hasn't really offended, although technically there had been a breach of security protocols; one where it might be resolved informally, and should nevertheless be recorded; and then a kind of third level where you actually hit that test on a reasonable belief basis and you are then duty-bound to report both to the individual and to the PCO.

Hon. Geoff Regan: I can envisage a situation where a company I dealt with on the Internet informed me that there had been sort of a breach and that I examined it and said okay, I was satisfied it was nothing too damaging and that I would waive my right to complain about it or to go through the whole process, but the question is whether people are properly informed.

Are there other views on this from witnesses today who would like to comment on this question about how to handle that?

● (1225)

Ms. Micheal Vonn: Perhaps in distinction from the view of some of our colleagues on the panel here, my view of what was happening with the recording obligation was that it was not to provide an onerous, bureaucratic nothingness; that it was actually one of those tools of reflection for the organization, in the sense that one piece of misdirected mail is human error, five pieces of misdirected mail is human error, but maybe 20 pieces isn't, and now you're starting to require some bureaucratic attention to systems. As an educative function—because you will, of course, be recording this, however informally it has occurred, even if it's very minor—it would be helpful reflection for organizations, again not punitively, but in order to appropriately assess practices.

That recording and that taking on of the obligation to essentially note even mere, technical, small, seemingly non-risk-based disclosures again helps reflect on practice in ways that we find could be educative.

The Chair: Thank you very much, Mr. Regan and Madam Vonn.

Now we will move to Mr. Carmichael.

Mr. John Carmichael: Thank you, Chair.

Welcome to our witnesses.

I'd like to begin with the Canadian Bankers Association. Feel free to determine who answers.

In your opening comments you talked about financial abuse, specifically of our most vulnerable. In your comments you said that PIPEDA limited you in much of what you would report when you saw a potential senior abuse or elder fraud, something going on that was inappropriate.

My understanding of Bill S-4 is that much of the remedy for this is now in place. I wonder whether you could talk to what works and what doesn't work to assist you so that your members can support and improve the situation of those most vulnerable clients.

Ms. Linda Routledge: The banks generally speaking would see potential or suspected financial abuse in the branches. It could be a client coming in with a caregiver or whoever and there being some kind of suspicious transaction. Right now, the first step of the bank would be to try to take that client aside so that they get them away from the suspected abuser, so that they can determine what the client wants to do. But in some cases that's not possible, and so we just have a suspicion.

Many times the amount of money may not be large in that instance, and that instance may not be fraud. We are constrained in being able to approach the police or the public guardian and trustee to ask for their assistance, because there is not a contravention of the law or fraud.

What we're looking for, and what Bill S-4 is giving us, is the ability to then escalate this matter and have it investigated further—because within the banks there is an escalation process—so that we can assess whether there is somebody else out there we can contact who would be able to help our customer avoid the abuse. It may be a parent, a sibling, or someone like that. We would assess and try to determine to the best of our ability whether that person is involved in the abuse—we recognize that in many cases it's a family member—and we would do our utmost to determine that the person we're contacting is not involved in the abuse.

That is where Bill S-4 would help.

Mr. John Carmichael: Bill S-4 provides that ability for you.

I think it's important, because this is an area we all know is growing—

Ms. Linda Routledge: Absolutely.

Mr. John Carmichael: —and when there is an opportunity for somebody to report, you want to know that the report is going to fall on ears that are able to listen and respond.

Going over to the Retail Council, I'd like to refer to your opening comments on consent in Bill S-4. In this paragraph you say, “We note that the bill contains a provision specifying that 'Consent is not valid unless how the information will be used is clearly communicated in language appropriate to the target audience.'”

Could you expand on that and talk to how that is going to benefit your membership?

Mr. Karl Littler: The section itself is relatively quiet on the intended protections and we've understood from the minister's comments in previous testimony that it's intended primarily to protect vulnerable individuals, and that's obviously a step that we wholeheartedly support.

We have heard from other witnesses that they see the section as superfluous and in fact, the current regime prospectively provides sufficient protection for vulnerable individuals. We're not experts in the operation of that but what we would say is this. We have no difficulty with the underlying premise of this. Where we would benefit, frankly, is from specification of the groups intended to be protected under this. I had named a few, but I'm sure that it is a non-exhaustive list. We would hope to see a regulatory power in there that would in fact specify those groups—again, in a non-exhaustive fashion.

I think for retailers the challenge that requires guidance, frankly, is this. There are a lot of scenarios here. Judging whether somebody is a minor will depend upon whether it's a face-to-face situation or an online transaction. In one case, you're presumably relying on whatever parental controls exist over smart devices and otherwise. If an individual in most cases indicates that they're over the age of whatever, you don't know with certainty whether you're getting what is really valid consent. In an in-store situation, it's easy enough to tell whether it's an eight-year-old but it may not be quite so easy to determine whether it's a person of the age of majority or if indeed that's the appropriate test in all circumstances. You're getting into a lot of subjectivity on issues of whether somebody has linguistic fluency, so a lot of what we're looking for in this is more specific guidance. We do find this provision general. We hope that there will be further development from it.

● (1230)

The Chair: Thank you, Mr. Littler.

That's all the time we had.

Now on to Madam Borg for five minutes.

[*Translation*]

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

I'd also like to thank the witnesses for joining us today.

I apologize for my tardiness. Unexpected things tend to come up a lot when you're an MP. My sincere apologies for missing some of the presentations and discussions. Forgive me if any of my questions have already been asked.

My first question is for Ms. Sali, but Ms. Vonn may also wish to answer.

Previous witnesses have told the committee that an oversight mechanism is needed in order to keep abuse in check when it comes to the disclosure of personal information without consent. Do you agree with that suggestion? What might such a mechanism look like, in your view?

[*English*]

Ms. Meghan Sali: I won't speak to what the mechanism could look like as I'm not an expert in that area. I definitely support the idea of a system to inform these people of what has gone on. If it doesn't put an investigation at risk—and this is obviously contained in the bill—we definitely believe that any disclosure of private information should be disclosed to the person whose personal information is being shared. As well, we also support the idea that if there is an investigation going on, where that sharing of information could possibly impinge on the investigation, the moment it no longer does, it should be shared with that customer as well. People's private information is, obviously, as previously stated, extremely revealing about their lives and about their personal activities. They have a reasonable expectation of privacy according to Spencer on this information. Definitely, we do think that there should be some sort of a reporting system in place so that people are aware of when their personal information has been shared and with whom.

[*Translation*]

Ms. Charmaine Borg: Thank you.

Ms. Vonn, would you like to comment?

[*English*]

Ms. Micheal Vonn: I can echo the concern about failure of notice. We don't have the system that you see in the United States where essentially your third party information holder becomes the guardian of the situation relative to protecting your rights. If this is your information, you are most likely to object to its use in a meaningful fashion if you have notice. I don't see that there's a way around that if we're serious about protecting individual rights.

● (1235)

[*Translation*]

Ms. Charmaine Borg: Thank you very much.

Ms. Sali, I'm going to read a comment made by your executive director. I'm going to read the quote in English as I don't have it in French. It reads as follows:

[*English*]

> ...this legislation, while welcome, does almost nothing to tackle the serious problem of ongoing government surveillance against law-abiding Canadians.

[*Translation*]

Since we are studying the bill before second reading, we have the ability to propose amendments to PIPEDA that don't necessarily appear in Bill S-4. I see that as a golden opportunity. Unfortunately, the government seems convinced that the bill is going to pass as is, regardless of the amendments suggested by all the witnesses. That's truly unfortunate.

In light of your executive director's comments, do you think the committee could improve certain aspects of the bill?

[*English*]

Ms. Meghan Sali: Yes, the amendment we'd like to see is the complete removal of non-notified voluntary disclosures. We think that voluntary disclosures, as Ms. Vonn has stated, put your telecom provider specifically in our interests in the position of being a gatekeeper and deciding what information they choose to reveal about you to any other company or in fact any other entity that is doing an investigation. As we've stated before, the scope of that investigation can include a number of different things, not just as we've noted before. It can expose Canadians to issues with copyright trolls, strategic anti-expression lawsuits, attempts at uncovering whistleblowers through specious lawsuits, and a range of other potential harms.

So the amendment that we'd like to see is the removal of non-notified voluntary disclosures.

[*Translation*]

Ms. Charmaine Borg: Thank you very much.

[*English*]

The Chair: Merci.

Now on to Madam Gallant for five minutes.

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

My first question is to the Bankers Association. Which elements of the proposed framework of the investigative bodies give cause for concern, which you outlined?

Mr. William Crate: In particular, it's (d.2), because it does restrict the sharing of information for prevention, detection, and suppression, to just fraud. By way of background, banks are under persistent and evolving threats. And the secret sauce, I think, in the security world within the banks is trying to prevent and detect, because by the time you have an occurrence, an event, or a crime, it's too late. A lot of effort is spent on trying to prevent and detect.

By way of example, we see a lot of organized crime paying attention to theft of credentials. That's theft of consumers' information. They're attempting to do that. You see that online yourselves, probably through phishing. That's not fraud. It's theft of information. If we can identify that earlier on by sharing information, whether it's IP addresses with each other that can be blocked, and then they can start to pay attention to accounts or information that may be at risk, I think that's much better than investigating and being reactive at the end. We're just concerned that the legislation may not permit that, going forward.

Mrs. Cheryl Gallant: So it's not that aspects of the new framework are of concern. It's what you just described.

Mr. William Crate: Yes, what we'd be asking the committee to consider for our industry is greater latitude. I would suggest swapping “fraud” for “crime” because then that covers everything.

Mrs. Cheryl Gallant: Thank you.

To the Retail Council of Canada, at the time of the review of PIPEDA, your organization stated that the current investigative bodies regime presents challenges to combatting organized crime in your industry. Would you elaborate on that, please?

Mr. Jason McLinton: I'll commence by saying that it was a couple of generations before my time. But, yes, I think that retailers, while not necessarily a driving force behind amendments to PIPEDA, would be generally supportive of anything that would allow for the speedy resolution of anything that was either occurring or about to occur. To perhaps restate what my colleague has said, the retail sector is generally supportive of this, primarily not just because of the specific provisions that are included in the bill, but because it supports PIPEDA, which retailers already have a very high level of compliance with, and that is working very well specifically because of its outcomes-oriented and technology-neutral approach.

● (1240)

Mrs. Cheryl Gallant: I will go back to the banking association. Financial institutions also provide insurance coverage for loans. What aspects of PIPEDA or Bill S-4 prevent the banking system from accessing the metadata or medical information on an insurance applicant under that same umbrella with the banks? The reason I ask is, the bank lender knowing a client's medical information could prejudice the lender. What you had stated previously is that you'd like to have more sharing of information to prevent a crime. How does the customer know that this barrier will not be crossed?

Ms. Linda Routledge: There is a specific provision in the Bank Act prohibiting it.

Mrs. Cheryl Gallant: Thank you. I have no further questions.

The Chair: All right.

Madame Borg, you have up to five minutes.

[*Translation*]

Ms. Charmaine Borg: Thank you, Mr. Chair.

Finally, I get the chance to ask my last question.

Ms. Vonn, my colleague, Ms. Nash, brought up the Spencer decision and the ensuing events in British Columbia, as well as the reactions of the commissioner and industry committee thus far. If I understand correctly, your organization participated in the review of the Personal Information Protection Act in light of the Spencer decision. Is that right?

[*English*]

Ms. Micheal Vonn: No, I'm sorry, we were not. We made a written submission, but we were not able to be there in person.

[*Translation*]

Ms. Charmaine Borg: But you did submit a written statement.

[*English*]

Ms. Micheal Vonn: Yes.

[*Translation*]

Ms. Charmaine Borg: We received a letter from the privacy commissioner indicating that Bill S-4 was based somewhat on B.C.'s model. That is what it was supposed to look like, but suggestions changed in light of the report. I think that calls into question the provisions in Bill S-4. Would you agree with that? Do you think we should find a way to bring the bill in line with the report recommendations as well, in order to achieve that alignment between the acts?

[*English*]

Ms. Micheal Vonn: Yes, I believe the coherence between the acts can be achieved if the analysis in Spencer is taken into account in relation to the voluntary disclosures.

I appreciate what the member was saying about there having been a year. We would like to move forward; it is long overdue. However, in the midst of that year we have had the decision that gives new import to the notion of what constitutes personal information and how we guard it. The most problematic provision that we keep hearing about is the voluntary disclosures outside of the areas of protecting vulnerable persons, fraud abuse, etc.

The sweep of this provision is something that in British Columbia and Alberta the privacy commissioners are now calling for reconsideration of. I think it's imperative that this committee essentially participate in this now-national debate on what the sweep should be. It would make sense to essentially sever that in this discussion so that the good, uncontentious parts of the bill could move forward.

[*Translation*]

Ms. Charmaine Borg: Thank you.

Ms. Sali, I believe your organization contributed to the review of the Personal Information Protection Act. Do you have any comments in that connection?

[*English*]

Ms. Meghan Sali: I am not entirely certain whether or not we proceeded in PIPA. That was a little before my time with the organization.

But if I may, I would love to mention, on the note that you just asked Ms. Vonn, that some have suggested that the approach in Alberta and B.C. has been totally fine and that there have been no problems with it. But one thing we've seen—and I'd like to echo Dr. Geist's testimony on this—is that the disclosure itself is not necessarily revealed to the person whose information has been disclosed. Often, the point is to disclose the information without the consent or knowledge of that individual, meaning that the affected individual would have a very hard time knowing that their information had been disclosed and in fact wouldn't be able to complain; or there would be no evidence of harm in that case, as they hadn't known.

I think the claims made by some that those B.C. and Alberta rules are not harming people is unfortunately untrue.

[*Translation*]

Ms. Charmaine Borg: Thank you.

How much time do I have left, Mr. Chair?

The Chair: You have a minute left.

Ms. Charmaine Borg: I have a question for Mr. McLinton and Mr. Littler.

Bill S-4 provides for a mechanism to notify individuals of security breaches. You appear to support that. The model proposed under Bill S-4 will require organizations to, themselves, determine whether the breach creates a risk of significant harm to the individual or not. Do you think it would be easy for your members to make that assessment? Do you expect to receive some support to ensure you are properly complying with the bill's provisions?

● (1245)

[*English*]

Mr. Jason McLinton: From the discussions we have had with our members, I think there is already, first, as I mentioned, a very high level of compliance with PIPEDA's requirements. It really comes down to a question of the size of the organization, as Mr. Littler suggested. We represent retailers from the very smallest mom-and-pop shops to the very largest general merchandisers and grocers. There are valuations already occurring at every level, and some more sophisticated than others, because at the end of the day the customers are the most valuable thing our organizations have.

That is happening now, but I guess with the smaller retail businesses it may be happening less formally. Compliance with PIPEDA is high, and reviews are already occurring with members.

The Chair: Thank you very much.

We will now move on to our final questioner, Mr. Lake.

Hon. Mike Lake (Edmonton—Mill Woods—Beaumont, CPC): I just have a quick question out of curiosity to start.

Meghan, you're from Vancouver, is that right?

Ms. Meghan Sali: I am.

Hon. Mike Lake: We have the B.C. Civil Liberties Association. Previously we had the B.C. Freedom of Information and Privacy Association. It seems like there is some sort of a core group from the Vancouver and Lower Mainland area. I'm curious about that. I did a little bit of research.

It's kind of interesting that Vincent Gogolek, who was here with us on Tuesday from the B.C. Freedom of Information and Privacy Association, was formerly the policy director of the B.C. Civil Liberties Association.

Philippa Lawson, who was also a witness on Tuesday, is listed on her LinkedIn page as a consultant, and her recent clients include the the B.C. Civil Liberties Association and the B.C. Freedom of Information and Privacy Association.

Ms. Micheal Vonn: That's absolutely correct. Privacy is a growing concern among Canadians, but the legal community with privacy expertise is a growing and evolving community. We are in fact few on the ground.

Hon. Mike Lake: And speaking as one voice, or several voices, at this committee, it seems.

Ms. Micheal Vonn: Not always speaking with one voice, but many times we do achieve a consensus.

Hon. Mike Lake: Okay. I found that interesting as we were listening.

To the banks, what I'm hearing is that your main complaint is that the investigative bodies section of the legislation is too restrictive. I think that's in proposed paragraphs 7(3)(d.1) and 7(3)(d.2). That's your main concern, correct?

Mr. William Crate: Yes, and in particular proposed paragraph 7 (3)(d.2). It may be less than what we can do today.

Hon. Mike Lake: That previous group that I just talked about all seemed to say with one voice that maybe it was the exact opposite.

I believe I've heard you all say, in almost the same terms, that that was the exact opposite.

We've heard others say similar things to what the bankers are saying. It seems like maybe we have a balance somewhere in between, which we see with legislation like this.

As for the retailers, you talked about proposed section 6.1 in what would be the new legislation. You're saying it needs some clarity concerning vulnerable persons. Is that correct?

Mr. Jason McLinton: That's correct. I would not say that's our primary concern though. To sum it up in a word, our primary concern would be undue administrative burden. That's the common thread, so that there's clarity around consent.

Hon. Mike Lake: In terms of the reporting requirements?

Mr. Jason McLinton: Reporting, record keeping, and all the other requirements that are mentioned.

Hon. Mike Lake: Interestingly, you're not the first ones to say that.

Those folks who are kind of speaking with one voice on the other side would say that it's the opposite, that we need more reporting and more notification.

Would you disagree with that?

Mr. Karl Littler: No. Let's make a distinction here between recording and reporting.

We have a concern about the recording burden. The section on recording is very strictly worded, which essentially means every breach of security safeguards. We can envisage a world in which that creates the burden to record breaches for which there's no foreseeable harm, and to create unlimited obligations—

● (1250)

Hon. Mike Lake: I only have a short period of time, but I want to ask you if the breaches that we're talking about, in your view, are things that should be avoided? Do you have no problem defining them as things we should avoid? Leaving a screen open with private information on it, I think was your example.

Mr. Karl Littler: For somebody stepping away from their desk to get a coffee, while some party is in the same room who may or may not have actually passed by that desk but with no certainty that the individual has done so, I think you have to have a materiality threshold.

Hon. Mike Lake: But it would probably be a good practice when you have personal information on your screen to close down your screen, right?

Mr. Karl Littler: Sure, it is a good practice.

Hon. Mike Lake: So as we try to establish that as a common practice across the board, to have some mechanism that simply records that it happened, as a reminder that we ought not do that—of course there's consultation going on in terms of what that's going to look like, and I'm sure you'll weigh in on that—might not be that onerous really. Eventually we shouldn't be doing that, right?

Mr. Karl Littler: I think we would differ.

I think that there probably is a threshold level below which—whether it's the period for which a filing drawer was open or a screen was left unattended—it actually might fall below a material level for the necessity of maintaining records, and in particular, one that also does not appear to have any time limitation on the requirement to maintain those records.

Hon. Mike Lake: I anticipate that, like the Bankers Association and everyone else, all of the witnesses here, you'll weigh in on the consultation process to make sure that the steps taken are reasonable.

The Chair: Thanks very much, Mr. Lake.

Thank you to the witnesses.

I usually hesitate to become involved at all, being the chair, but I want to ask the Bankers Association whether there is a regular relationship presently with the Privacy Commissioner such that—not, obviously, on a case-by-case but on an aggregated basis—there is a sharing of aggregate data on a quarter or half a year's investigations concerning how those have proceeded and how people's personal information has been safeguarded.

Do you have that kind of regular reporting aspect relationship with the Privacy Commissioner's office?

Ms. Linda Routledge: The banks' compliance divisions have a very close relationship with the Privacy Commissioner's office. Many times, when they have a question about compliance, they will talk to that office.

As an association, we host an annual meeting with the regulator so that we have the opportunity to exchange information with them. But the banks on a regular basis, as a breach may happen—in the rare instances when one does happen—are certainly in touch with the Privacy Commissioner's office so that they are aware of what is happening and are able to monitor what is going on and give advice as to how we can handle it.

We participated in the development of the Privacy Commissioner's guidance on breach reporting and notification. The banks certainly follow that guidance.

The Chair: I ask the question because it's a substantial trust that you have, and I also know that you have a substantial responsibility because of the nature of crime these days and the innovation that those who want to perpetrate such acts come up with on a day-to-day basis. I just wanted the committee members to hear briefly about what that relationship is.

Thank you very much, colleagues.

To our witnesses, thank you very much. Again I extend to you the regrets of the committee that we were held up by the due process of democracy in the chamber.

We're adjourned.