HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Industry, Science and Technology

INDU • NUMBER 033 • 2nd SESSION • 41st PARLIAMENT

EVIDENCE

Thursday, February 5, 2015

Chair

Mr. David Sweet

Standing Committee on Industry, Science and Technology

Thursday, February 5, 2015

● (1100)

[*English*]

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

Welcome to the 33rd meeting of the Standing Committee on Industry, Science and Technology.

We are beginning our study on Bill S-4, an act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another act.

Before us we have the Honourable James Moore, Minister of Industry.

I'll also go ahead and introduce the department officials, as well—Mr. John Knubley, deputy minister; Kelly Gillis, associate deputy minister; and Chris Padfield, director general, digital policy branch. I understand, Mr. Knubley, that in the second half you'll have opening remarks.

But for now we will begin.

Minister, if you would begin your opening remarks, and then we'll have our usual rounds of questions.

Hon. James Moore (Minister of Industry): Thank you very much, Mr. Chairman, and I appreciate the opportunity to come back, as you said, with my officials to talk about Bill S-4, the digital privacy act, which for me is a very important piece of legislation for a number of reasons: the context of the legislation in terms of Canada's digital policy moving forward but also our responsibility as a government, as a Parliament, to update our privacy legislation to protect Canadians.

But before I do that, I gather there were some changes in the committee membership, so I want to congratulate those of you who have been tasked to come onto this committee. As you know, the Department of Industry...and therefore your oversight of our activities, your advice, and constructive criticism, are of course an important part of our parliamentary function. To those of you who are on the committee, I look forward to working with you over the coming months as we move forward on pieces of legislation like this one here.

[*Translation*]

Thank you, Mr. Chair, for inviting me to appear before the committee today to discuss an important bill, the Digital Privacy Act, which is intended to better protect Canadians' personal information online.

[*English*]

You know, our government is focused on the mandate that we were given by Canadians back in 2011, to create jobs, focus on a growing Canadian economy and, as Minister of Industry, to move forward with an effective digital policy for Canada.

Also, we know that any government's plan that is centrally focused on the economy must of course have a robust engagement to strengthen Canada's digital economy. That's why last year I unveiled Digital Canada 150, our government's plan that sets clear goals for a connected and competitive Canada. It will help Canadians participate and succeed in our digital economy. One of the key pillars under Digital Canada 150 is the need to protect privacy.

The digital privacy act is an essential part of that goal. Our government understands that a strong digital economy requires strong protections for Canadians when they surf the web and when they shop online. The digital privacy act will modernize Canada's private sector privacy law by introducing important new protections for Canadians online. It sets clear rules for how personal information can be collected, used, and disclosed. It requires organizations to tell Canadians if their personal information has been lost or stolen and imposes heavy fines on companies that deliberately break the rules. It gives the Privacy Commissioner of Canada more power to enforce the law and to hold offenders to account. The bottom line is that it delivers a balanced approach to protect the personal information of Canadians, while still allowing information sharing to stop illegal activity when it occurs.

These are much-needed changes to Canada's private sector privacy law, the Personal Information Protection and Electronic Documents Act, or more commonly known as PIPEDA. PIPEDA "sets out the ground rules for how private sector organizations... collect, use or disclose information in the course of commercial activities" across Canada. This should not be confused with the Privacy Act, which deals with how the Government of Canada handles the personal information of Canadians.

Let me share with the committee four areas where the digital privacy act will significantly improve PIPEDA.

First...data breaches. Unfortunately, this is an all-too-familiar topic for Canadians in our digital age.

● (1105)

[*Translation*]

It may surprise the committee members to learn that, under the current legislation, businesses are not obligated to notify Canadians of security breaches involving data under their control.

In other words, if a company's data is compromised and a hacker gets a hold of your credit card number, the company is not under any obligation to notify you. That's a serious problem.

[*English*]

Last December, for example, Target revealed that a data breach had compromised millions of its customers' credit and debit card information. In September, Home Depot announced that a data breach perpetrated by unknown hackers left as many as 56 million debit and credit card customers across North America vulnerable to fraud. On October 10, Kmart disclosed, in the United States, that almost all of its 1,200 stores throughout the States had been attacked by hackers, putting credit card and debit card details of customers potentially in jeopardy. Later in October, Staples announced a suspected breach of its customers' credit card and debit card information as well.

Canadian online consumers need stronger laws to protect them from similar fraud here. The digital privacy act will make it mandatory for an organization to tell individuals if their personal information has been lost or stolen and whether or not it puts them at any risk.

[*Translation*]

Under the Digital Privacy Act, organizations will be required to notify individuals whose personal information has been lost or stolen and let them know whether they are at risk of harm as a result.

Companies will have to inform Canadians of the steps they must take in order to protect themselves, such as changing their credit card PIN or email password. These are crucial safeguards to protect Canadians, and yet they are not currently in place.

[*English*]

The digital privacy act has been praised by consumer rights groups and those in the retail industry for its balance. The Marketing Research and Intelligence Association has said that they support the mandatory breach notification requirements that are in the bill. The Canadian Marketing Association has said that they support the changes to breach provisions.

The digital privacy act will make it mandatory that organizations also report these potentially harmful breaches to the Privacy Commissioner. When there's a privacy breach, not only is the individual informed by law; the Privacy Commissioner is also informed by law. In fact it will be mandatory for all organizations to keep records of all data breaches as well. If the Privacy Commissioner makes a request for these records, they must be handed over. Once law, organizations that deliberately cover up privacy breaches and destroy records will face fines of up to $100,000 for every person or client that they intentionally fail to notify.

The Office of the Privacy Commissioner of Canada is on the record as supporting these amendments as being in the best interest of Canadians. In addition, in my home province, the B.C. privacy commissioner has also recommended to their provincial government that they adopt the same approach that we have taken in Bill S-4.

Second, our digital privacy act clarifies the rules around obtaining consent to protect vulnerable Canadians online, particularly children and seniors, when companies ask to collect and use their personal information. For example, when the owner of a website for children wants to gather information about visitors to the site, the owner will need to use language that a child could reasonably be expected to understand. If the child can't be expected to understand how the information will be used, the child's consent would not be deemed valid. The owner would need to get consent from a child's parent.

This amendment makes it clear for companies how consent works under the act. This is something about which there has been confusion. This legislation does make it clear so that they can adopt best practices.

If an organization is targeting a product or service at a particular segment of the population, such as children, then any attempt to obtain consent must be adjusted accordingly.

Again, Mr. Chair, the Marketing Research and Intelligence Association agrees with these changes, saying that it “fully supports the provisions in Bill S-4 which provide added clarity for organizations when they seek the valid consent of an individual”. Given the increased use of smartphones and tablets among young people, the stronger rules included in this bill will make sure that individual Canadians, especially children and adolescents, can fully understand the potential consequences of sharing their personal information.

● (1110)

[*Translation*]

The Digital Privacy Act further protects Canadians by setting out certain exceptions in which personal information can be shared when it is necessary to protect an individual from harm.

In certain situations, it is in the public interest to share an individual's personal information without their consent. For instance, the information could be shared for the purpose of reuniting parents with a sick or injured family member when they are otherwise unable to contact that family member.

[*English*]

Another example would be by allowing banks and financial institutions to share personal information with law enforcement or family members when they suspect cases of financial abuse, especially to protect against elder financial abuse. The Canadian Bankers Association has applauded the amendments contained in this bill that would allow banks and financial institutions to advise public guardians, law enforcement, or family members when they have evidence of financial abuse, particularly of elders.

Mr. Chair, I want to pause here to address one issue that was raised in question period when this bill was debated in Parliament before being referred to this committee. That's with respect to the Supreme Court of Canada's decision in the Spencer case. Some have suggested that PIPEDA, and the digital privacy act by extension, in some way may violate the Charter of Rights of Canadians and need to be changed.

This is patently false. PIPEDA does not create any search or seizure powers for law enforcement. It does not require companies to hand over information to law enforcement. It only allows private sector organizations to voluntarily provide information to law enforcement and government agencies when they have the legal authority to obtain it. This decision does not mean that PIPEDA or Bill S-4 is unconstitutional, and no changes to Bill S-4 are required in that regard.

Some privacy advocates, including the Privacy Commissioner, have called for greater transparency on the part of businesses with respect to how often and under what circumstances they provide information about their customers to police.

Openness, of course, is one of the key principles underscoring PIPEDA, and nothing in PIPEDA prevents Internet service providers or other companies from publishing such transparency reports. I'm pleased to see that over the past year a number of Canadian companies have done just that.

[*Translation*]

Lastly, under the Digital Privacy Act, the Privacy Commissioner will have new powers and tools to enforce the act.

[*English*]

The former interim Privacy Commissioner supported this legislation when she said that the digital privacy act "will strengthen the privacy rights of Canadians. We welcome proposals to introduce a mandatory breach notification regime and the compliance agreement provisions that will make it easier for our office to ensure that companies meet the commitments that they have made. We strongly support these provisions."

I would point out as well that before we drafted this legislation and before it was presented to the Parliament of Canada, we consulted with the Privacy Commissioner's office to ensure that this legislation satisfied their concerns with regard to privacy and that we were taking all reasonable steps to ensure that concerns that had been raised in the past about this type of reform were recognized and considered in the drafting of this legislation. That's why I'm grateful for the Privacy Commissioner's support of this legislation.

Under the digital privacy act, the commissioner will now be able to negotiate voluntary compliance agreements with organizations to hold them accountable for their commitments to correct privacy problems. In addition, the Privacy Commissioner will now have one year instead of 45 days to potentially take organizations to court if they don't play by the rules. The digital privacy act will also give the commissioner more power to name and shame, or to make information public where organizations do not play by the rules. This change will make sure that Canadians are informed and aware of issues that affect their privacy. Organizations either comply with the law or they will face public scrutiny.

Our government is balancing the privacy needs of Canadians and the ability of businesses to legitimately access and use personal information in their day-to-day operations. The Canadian Marketing Association has expressed their support overall for this legislation when they said that it "supports the government's effort and this bill to update Canada's private-sector privacy law".

The Canadian Bar Association said, "We express our support for the digital privacy act".

As we move forward with the implementation of the act, I look forward to working with the Privacy Commissioner to provide all the necessary clear and practical guidance to help with full compliance. The digital privacy act, as I said, is a much needed update to Canada's private sector privacy law, particularly in our modern digital economy.

[*Translation*]

The bill gives Canadians the assurance that their information will be equally protected, no matter who they chose to do business with in Canada.

Thank you. I would be happy to answer any questions the committee members have.

● (1115)

[*English*]

I would certainly like to again thank committee members for their consideration of this legislation. As you know, it's Bill S-4, not C-4, and this legislation has already been adopted by the Senate. It received quite deep and thorough study on the Senate side. This was treated, I think, with a great deal of respect and the necessary intensity, and I was pleased that it was adopted by the Senate. I look forward to this committee giving it the scrutiny that it deserves.

Thank you.

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

We'll go into our rounds of questions now. Colleagues, a couple of things. We have enough time for five minutes for each member and that's really it. So please don't take it personally if I have to interrupt you. I'll do it with as much dignity as I can. Also, at the end of the second hour, we will take a couple of minutes for a small piece of business. We'll go in camera for that.

So now we'll begin with Mr. Lake for five minutes.

Hon. Mike Lake (Edmonton—Mill Woods—Beaumont, CPC): Thank you, Mr. Chair, and thank you to the minister for coming here today.

I remember before you were the Minister of Industry, you were the Minister of Canadian Heritage, and we had the opportunity in this committee, or in a joint committee, to go through the copyright legislation that we did. One of the things that a lot of people praised the government for at the time was really finding a balance with the copyright legislation that we put forward.

I hear you use that word time and time again in your presentation here, the importance of finding a balanced approach here because there are so many different directions that you could go with privacy. Maybe you could elaborate a little bit more on the balances that you struck here in putting this legislation forward.

Hon. James Moore: Sure. I don't know if “balance” is maybe necessarily the right word, but the digital economy to thrive. I suppose the balance is found in not putting forward legislation that would have a chill in terms of firms aspiring to fully engage the digital economy and thinking that the Government of Canada was being too onerous in our expectations of what firms have to engage in in terms of responsible behaviour and protecting the privacy of Canadians. We want to have a balance. We don't want to be a barrier. We want to spur on greater adaptation of digital technologies and the digital environment, while at the same time recognizing that Canadian consumers deserve to be protected, not just at the same level as other countries around the world. We want to actually exceed other countries' approaches to these things and to give Canadians the best possible regime in the world, which is why there has been a great deal of consultation.

If I may say, if there's a criticism to be levied, it's that this legislation has taken too long to come forward, but we are here now and this legislation will be meaningful in striking the appropriate policy framework that will benefit Canadians.

Hon. Mike Lake: You spoke earlier in your remarks about the Digital Canada 150 strategy and the importance of that strategy moving forward. I think everybody at this committee recognizes the importance of that.

How important is getting the privacy piece right in this piece of legislation to advancing the Digital Canada 150 strategy?

Hon. James Moore: Digital Canada 150 has five pillars to it, 39 specific action items, and one national policy for all of Canada.

The first of the five pillars is connecting Canadians. It's making sure that we're all bound together and fully participating, as the second largest country in the world in size but 37th largest in terms of population. In a wireless sphere, with our connecting Canadians program and our investment on a P3 basis in infrastructure all across the country, it's that all Canadians are connected going forward. As well, of course, with our wireless policies, it's that we have world-class connectivity and competitive pricing with adequate competition, which is why we've taken the approaches we have on spectrum auction and spectrum transfer policy.

The second pillar is the digital economy. You'll remember when we first did our digital policy efforts in our first term in government, we talked about a digital economy strategy. Well, at the time, it was around the margins of the worst recession since the Second World War, and, of course, everything had the language of an economic policy and economics. But the truth is that a digital economy strategy, in my view, is a bit too narrow of a lens to put on a broad digital policy for a country. That said, there are specific measures that a government can take in order to ensure that the digital economy is moving forward. This speaks to it a little bit, but there are other measures as well.

One pillar is connecting us. The second pillar is the digital economy and the opportunities that exist within it. A third pillar is making the government more digital than ever before: the Open Data Institute that we have, the OpenScience initiative, making sure that government information is more accessible online than ever before, and taking those initiatives that Tony Clement, as President of the Treasury Board, has tackled.

The fourth pillar is protecting Canadians online, so: connecting Canadians; digital economic strategy; more digital government than ever before; and protecting Canadians online, which this legislation is central to.

The fifth and the final pillar is the one that I find most fun and interesting. Once you connect everybody, once you've made it more secure, you're taking full advantage of the digital economic opportunities, and the government is walking its talk and hopefully adopting the more digital approach to the way it does everything, then you breathe life into all of this with digital Canadian content. A central point to all of this is pushing our museums to be more digital, ensuring that the public broadcaster, the Canada Council for the Arts, and everybody who is engaged in telling Canadian stories to Canadians about Canada, our history and aspirations and all of these things. This country only survives if we have better understanding of our history, better opportunities to talk about our aspirations for the future. Breathing life into the content side is the fifth and final pillar.

None of these pillars stand on their own. If any one of these pillars was the entirety of the digital policy, it would lack comprehension. This is essential for us to move forward.

● (1120)

The Chair: Thank you, Minister.

That's all the time we have.

Madam Borg.

[*Translation*]

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

Minister, you said that Bill S-4 did not violate the Constitution and that the Supreme Court's decision in the Spencer case did not apply to the provisions in the bill.

Did I understand you correctly?

Was any research done in that regard, further to the Spencer decision?

Hon. James Moore: Yes, my department made certain that the bill respected the decisions of the Supreme Court of Canada, as well as the government's other obligations, including the obligation to bring forward legislation that respects the Constitution and legislation already in place.

Chris may want to provide a bit more detail on the Spencer decision and the implications for the bill.

[*English*]

Mr. Chris Padfield (Director General, Digital Policy Branch, Department of Industry): Thank you, Minister.

To be quite clear, the Spencer decision, paragraph 71, was quite clear that PIPEDA creates no new search or seizure powers for law enforcement. The way that PIPEDA would function is to reflect the authorities that are elsewhere for police. Section 7(3)(c.1) identifies the circumstances in which companies can voluntarily provide information to law enforcement where they have a lawful authority to receive it. The Spencer decision clarified what that lawful authority means. It meant either that there is a common law authority where there's no reasonable expectation of privacy, or in circumstances where there is a reasonable expectation of privacy that there's a reasonable law, that police have a warrant, or that there's exigent circumstances. PIPEDA reflects all of those circumstances, and the Supreme Court decision was quite clear that it has no bearing on PIPEDA itself.

PIPEDA does not create search and seizure powers for law enforcement.

[*Translation*]

Ms. Charmaine Borg: You would agree, though, that the Spencer decision makes clear that Internet users have a reasonable expectation of privacy when online, would you not?

[*English*]

Mr. Chris Padfield: It did in that very specific circumstance where the police were searching for...they had an IP address. They understood that the individual in that case, Mr. Spencer, had been uploading and downloading child pornography. In that circumstance they had the IP address, but they didn't know his identity. In that circumstance they went forward and asked the telecommunications provider to provide the basic subscriber information. Through the court process they came back and said that collection of information, the basic subscriber information and that IP address combined, amounted to what would be a search under the Constitution. In that circumstance they didn't have common law authority that they were relying on to obtain that information. They required a warrant in that specific circumstance because his Internet browsing history and other things related to his IP address provided them with intimate biographical details that went beyond the needs of that circumstance. A warrant in that specific circumstance was needed. They could not rely on common law authority as they had tried to.

● (1125)

Ms. Charmaine Borg: You say that the Spencer decision did create a certain clarity or ambiguity in respect to how you would interpret it around what is a lawful authority. In PIPEDA, we do allow for government institutions to make requests to Internet service providers. Are you suggesting that it is the opinion of the industry that a lawful authority would include a government institution?

Hon. James Moore: Again, only with the consent of courts. The government cannot do it without consent. The legal framework still exists.

Ms. Charmaine Borg: Okay, thank you.

[*Translation*]

I'm going to move on to another aspect of the bill.

As you said in your opening remarks, the purpose of the bill is to better protect Canadians' personal information, and that's an important step. With the bill having the title it does, one would think that the purpose was really to protect Canadians' personal information. Clauses 6 and 7, however, create new exceptions, under which organizations can share an individual's personal information without obtaining their consent or notifying them.

Do you think that is a good way to better protect Canadians' privacy?

[*English*]

Hon. James Moore: No. I think that overstates it. I think the legislation is quite clear. We put forward this legislation after consulting with the Privacy Commissioner, as you know. The mandate of the Privacy Commissioner is certainly to err on the side of caution, not only in terms of the mandate of the Privacy Commissioner but in the approach that he or she has over time—

[*Translation*]

Ms. Charmaine Borg: I would just like to point out that the Privacy Commissioner said he did not support that provision.

[*English*]

The Chair: Just briefly, Minister, please.

Hon. James Moore: As I said in my remarks, I think this strikes the right balance. I don't think Ms. Borg has the correct interpretation of either the Spencer decision or the legislation.

The Chair: Thank you.

Mr. Carmichael now. Five minutes only, please.

Mr. John Carmichael (Don Valley West, CPC): Thank you, Chair. Welcome to the minister and his officials.

Minister, I agree with you with regard to PIPEDA and this legislation being long overdue. Clearly, technology has advanced at such a pace that legislation must catch up with so much of what can occur within the technology and the world around us today.

An area of concern to me as a grandparent is with my young grandchildren who, when I watch them on technology today, function much faster and ably as they work their way through their iPads or whatever it might be. One of the concerns I have is how this bill will protect my grandchildren and those of all Canadians. Can you expand a little bit on your opening comments in that regard and what penalties exist for those who break that trust?

Hon. James Moore: Your caution is right. I know you just became a grandfather, I think again, very recently. Congratulations on that.

This is obviously an important part of the government's obligation as everything shifts to digital, and everybody is doing everything with tablets and smartphones at their convenience.

The approach to the legislation is about the consent that's offered. As you know, in the world of big data and in the world of collecting that data, we need to make sure children understand the risks that are online. Not all of this, of course, can be done or frankly should be done as a quasi-parenting function of the government. We all have an obligation to protect ourselves, those we care about, and the broader society.

But we also have institutions and bodies, such as the Privacy Commissioner, the Government of Canada, through legislation like PIPEDA, or through privacy legislation that we have as the Government of Canada more broadly when we're dealing with citizens' interaction with the government to ensure we are protected. This legislation takes steps to ensure, when a child is online and giving consent or sharing information, that the language used is, frankly, plain-spoken and can reasonably be expected to be understood by a child. I know that's a very subjective way of saying it.

Let's say, for example, that a child goes onto a website of a cartoon figure and provides his personal email address, home address, or phone number. That information was drawn out of the child. He's using the website in a way that was duplicitous or not clear, or the child might have given that information in a way...that was duplicitous, and a parent later finds out about it. That is reported to the Privacy Commissioner. The Privacy Commissioner can then take action. The entity putting up that website is forced to immediately take down the website and re-offer that information in a more responsible way.

Yes, there is some subjectivity in all of this, but the approach we've taken is to entrust the Privacy Commissioner with this approach, based on experiences in other jurisdictions around the world, in the trial and error they've had in trying to put in place this kind of public policy. Those firms that don't comply with this certainly can face penalties from the government, or by extension the Privacy Commissioner, and certainly some name-and-shame capacities. You would think that some of these firms, if they're engaged in this kind of behaviour.... If the Privacy Commissioner were to issue a report saying they were engaged in an approach of data collection about our kids that is unsafe and that violates the privacy of our kids, I think that would be a death sentence to that firm.

The powers that are in here are incredibly powerful in the free market for firms that are engaged in this kind of a process. The fine, as my deputy has just signalled to me, is $10,000 up to $100,000 either per data breach or per abuse of the privacy of individuals, including kids.

● (1130)

Mr. John Carmichael: Good. Thank you.

Maybe we will just move to the other end of the spectrum and talk about seniors. I've run many seminars and round tables relevant to financial abuse, senior abuse, elder fraud, etc. I wonder if you could quickly talk to some of these issues as well, and how this bill will protect our seniors.

Hon. James Moore: Yes. It's a difficult part of the legislation. I would suggest—far be it from me, committees are masters of their own agendas in how they move forward—that this is one piece of the legislation where there is, I think, a reasonable debate on the best way to move forward. The way we've put it forward in the legislation is obviously the way we've arrived at what we think is the best balance.

My own family experienced in years past the financial abuse of my grandmother by a caregiver. This is not an uncommon problem.

In the legislation under the current law, for example, if banks or financial advisers suspect that their client, a senior, is a victim of financial abuse, they are currently prevented from notifying proper authorities, in part because of the privacy protections. This legislation clarifies that.

The grey area is that very often the financial abuse is happening within the family. This is where it might be useful for this committee to draw in some witnesses to give the actual point-counterpoint, because it's a legitimate debate. When, for example, financial institutions, banks, clearly see or they're quite suspicious that there's financial abuse happening to a senior, if their only course of action is to inform the family, and they can't inform the authorities because of our current privacy law, that will not actually protect the senior, because it's often a family member doing the abuse.

I know that some have said that this is a hole in the legislation because it provides a financial institution the ability to inform authorities about suspected abuse of the elderly. It's true that we do create that provision, but it's because very often—I don't know what the proportion is—the financial abuse is happening within families. To inform the family would allow them to probably cover their tracks and get away with the abuse of a senior, and that's something we want to stop.

The Chair: Thank you, Minister.

[*Translation*]

Mr. Dubourg, you have just five minutes.

Mr. Emmanuel Dubourg (Bourassa, Lib.): Thank you, Mr. Chair.

Good morning to you, to the minister and his officials, and to all my colleagues around the table.

We are talking about Bill S-4. In today's technological environment, it is indeed important to bring forward measures like these, but it is also important to make sure that personal information is well-protected.

Let's get right into it and look at new section 7(3)(d)(*i*), which deals with exceptions to consent requirements. It says that the information can be disclosed if the organization "has reasonable grounds to believe that the information relates to a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed".

How can an organization determine the relevance of the information it is sharing to a federal or provincial contravention, all the while protecting individuals' rights?

● (1135)

Hon. James Moore: That's a good question.

In our view, Bill S-4 clearly defines the obligations organizations and businesses are under in that regard. Once the bill comes into force, if any organizations have questions or need clarification, they can certainly speak to the people in my department or contact the Office of the Privacy Commissioner of Canada.

We introduced this bill to address the need to balance the rights of Canadians and the right to privacy. As I said in answer to Mr. Lake's question, we need to make sure that we are not creating barriers for organizations and businesses wishing to fully participate in the digital economy.

Mr. Emmanuel Dubourg: Very well. Thank you, minister.

We're talking about disclosing information. How is it possible to know whether the reason for disclosure is valid or not? The individual concerned doesn't know that the information is being shared between organizations. How is it possible to determine whether the reasons for sharing the information were valid?

Hon. James Moore: That's a good question.

It's not always easy to figure out. Hence the importance of making sure that, whenever you give your credit card number to a supplier online, you have to read all the fine print, so to speak, because, at the end of the day, you are giving an organization your legitimate consent to share your personal information.

It's vital that, when using technology, consumers be extremely careful with their personal information. For that reason, Bill S-4 has a provision meant to protect young people, because they are the most vulnerable to these kinds of violations.

It's challenging for a government to put in place laws and regulations to protect people in their online communications. We believe this legislation gives the commissioner the powers needed to protect Canadians.

It's an ongoing debate in society and the media, not to mention within families. Whenever a breach of personal information occurs, we have to try to understand what went wrong and adopt new measures to protect individuals.

Mr. Emmanuel Dubourg: Minister, I realize that this is a piece of legislation and, as such, has to be somewhat general in nature. The bill refers to prospective breaches, however. Don't you think including future data breaches gives the bill an overly broad or general scope?

Hon. James Moore: No, I don't. I think it's appropriate.

We can't predict what direction the online world will take. The bill contains rules and principles that will remain valid. I have no doubt that, down the road, after its implementation, the legislation will undergo a review. At that point, we'll be able to tell whether it's doing the job and protecting Canadians' interests.

[*English*]

The Chair: Now on to Madam Gallant for five minutes.

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

Minister, this bill's supposed to reduce unnecessary red tape by making businesses access their information during their normal activities.

Can you explain how this occurs?

Hon. James Moore: Sure. As you said, we've undertaken both with Minister Bernier as small business minister and, prior to that, Minister Rob Moore when he was minister of small businesses, the red tape reduction action plan, a bold name for a very important initiative for small businesses to ensure they are not overly burdened.

This legislation provides changes because we need to recognize companies need to have access to and to use personal information to conduct legitimate businesses.

Up until now there has been a lack of clarity, which is part of the reason small business organizations were brought into the process of drafting this legislation, hearing their concerns about how we can move forward.

You can imagine the massive shift that is happening. We see it with retail stores and the way in which we're advancing their businesses, especially if you're a small business.

If you're going to reorient your business and shift much of your sales regime to online sales, you need to make sure not only do you have the best, most efficient, and most up-to-date systems of engaging with consumers, but you're doing it in a safe and responsible way. As I said, if you have one data breach in a small firm, and that word gets around, and it goes viral electronically, your business is shuttered. It's toxic.

Therefore firms have to do their due diligence. We as a government have to be part of that, not just in imposing more and more obligations onto firms of what you must and must not do, which would cause small or medium-sized enterprises that are aspiring to be bigger and to engage in bigger markets, including markets overseas.... With the passage of the Canada-Korea Free Trade Agreement and the coming of the Canada-Europe free trade agreement, as small and medium-sized enterprises aspire to be global in their reach, they need to make sure their systems are fully secure and safe and protecting individuals. Not only in the practical application of law like this in terms of regulation, but also reputationally, we need to make sure Canadian firms are seen globally as operating within a regime that is world-leading in the protection of the privacy rights of individual consumers.

That's what we aspire to do. We think we do this in a very clear and straightforward way that reduces red tape—I know red tape is a bit of a catch phrase—in that sense by making the rules clear for small businesses that wish to further engage in the opportunities of doing commerce online.

● (1140)

Mrs. Cheryl Gallant: With respect to the comments you made pertaining to the Charter of Rights, when a data breach occurs through hacking, it's a criminal offence, and you're confirming that a warrant will be required to investigate a cybercrime.

Hon. James Moore: That's correct.

It would depend on the context of the data breach, for example, but yes, the current procedures that require the government and police forces to access this information would stand.

Mrs. Cheryl Gallant: So this applies only to Canadian companies that are physically situated here?

Hon. James Moore: No, it applies to firms that have access to Canadians' data.

Chris, I'm sure I'm lacking clarity on this.

Mr. Chris Padfield: With respect to the data breach provisions, if a company uses Canadian data, the provisions will apply.

Mrs. Cheryl Gallant: Canadians don't necessarily know if the company with which they are doing their online shopping is situated in Canada. Many companies have a .ca even though they are somewhere else.

How do they know they are PIPEDA protected?

Mr. Chris Padfield: By definition, by doing business here in Canada they have to comply with the privacy law.

As part of the aspect of the name-and-shame powers, the commissioner had gone after large Internet corporations before. She dealt with Facebook, Google, and what have you, and went after them under PIPEDA because they operate here.

One of the expansions of the name-and-shame powers that the minister mentioned gives a commissioner even further reach to be able to publicly state when they have identified issues that have gone on, that these things are happening, and even if they are outside Canada and they are affecting Canadians, the commissioner will be able to—

Hon. James Moore: Yes, and the lens is inverse. We're protecting Canadians. It's about protecting Canadians and their right to have their information protected by firms. That's what it's about. It's not about the firm. It's about the rights of Canadians.

The Chair: We go to Ms. Nash, for five minutes.

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

Welcome again to the industry committee, Minister, and your top officials.

Many Canadians broadly welcome action by the government on digital privacy. It has certainly been long overdue. Canadians do want enhanced protection for their digital privacy.

I want to, as some of my colleagues have, ask questions about certain parts of the bill that many consider to actually threaten Internet and digital privacy of Canadians. I'm specifically referring to clauses 6 and 7, which add to the exemptions in which personal information can be collected, used, or disclosed without consent or the knowledge of the individual. Testimony at the Senate hearings on this bill raised these concerns.

A member of the Canadian Bar Association on the national privacy and access law section said:

> We are concerned that, as drafted, the proposed PIPEDA amendment, section 7(3)(d.1) and (d.2), is unnecessarily broad and would permit disclosure without consent in an inappropriately broad range of circumstances.

The office of the Privacy Commissioner said:

> First, we believe that the grounds for disclosing to another organization are overly broad and need to be circumscribed, for example, by defining or limiting the types of activities for which the personal information could be used. The proposed 7(3)(d.2) would allow disclosures without consent to another organization to “prevent fraud”. Allowing such disclosures to prevent potential fraud may open the door to widespread disclosures and routine sharing of personal information among organizations on the grounds that this information might be useful to prevent future fraud.

Minister, are you of the opinion that sharing personal information without the knowledge of consent between businesses is helping the privacy of Canadians?

● (1145)

Hon. James Moore: Not without the consent of the individual, which was part of my response to our Liberal colleague about the consent. People have to consent in order for their information to be shared.

Some of the particular circumstances where we allow for sharing of information business to business, for example—separate from the government, where we allow it to happen—are for the examples that I've described, such as elder abuse. This has been called for and asked of the government.

You've listed some of the firms that have raised some concerns about the legislation; many of the people you cited still think the bill should be passed. I can certainly give you a long list of people who have given us quotes saying they're very thankful that the government has put in place this kind of flexibility in the legislation, so that we can prevent things like elder abuse, financial abuse, and that we can protect our children. Very often we do have to have the sharing of information between firms, so that they are doing their due diligence and protecting consumers from privacy breaches.

Ms. Peggy Nash: Thank you, Minister.

I have such a short time. I just need clarification because, if I understand the law correctly, section 7.2(1) says:

> In addition to the circumstances set out in subsection 7(2) and (3) for the purpose of clause 4.3 of Schedule 1...organizations that are parties to a prospective business transaction may use and disclose personal information without the knowledge or consent of the individual if

And then it has a long list that I won't read. For example:

> (a) the organizations have entered into an agreement that requires the organization that receives the personal information
>
> (i) to use and disclose that information solely for purposes related to the transaction,
>
> (ii) to protect that information by security safeguards appropriate to the sensitivity of the information, and
>
> (iii) if the transaction does not proceed, to return that information to the organization that disclosed it, or destroy it, within a reasonable time; and
>
> (b) the personal information is necessary
>
> (i) to determine whether to proceed with the transaction, and
>
> (ii) if the determination is made to proceed with the transaction, to complete it.

There are other sections that I could read. I guess my question is, where there are these warrantless disclosures of personal information —that's basically personal information-sharing between companies —is the minister open to any amendments to either remove some of the sections that have really been troubling, or perhaps to put in some checks and balances in order to ensure that these clauses are not abused? I think there are some very good things in this bill, but there are some legitimate concerns that they may be overly vague or broad.

● (1150)

The Chair: We're about one minute over, so I'll just take it off for the answer.

Go ahead, Mr. Knubley.

Mr. John Knubley (Deputy Minister, Department of Industry): I think this is an area of important clarification. There may be two sets of points, and I'll ask my colleagues to help me on this.

First, I think we believe, as administrators, that we are not opening the door wider in this regard. What we are actually doing is bringing PIPEDA in line with the practices of other provinces like Alberta and B.C. here. Currently, we apply regulations in these specific areas of non-consent, and we're moving away from that to a series of tests we think are as rigorous as the regulation.

In terms of Bill S-4 itself, there is a series of amendments relating to business contact information and business transaction, for example, businesses in a merger, an acquisition; if it's specifically related to a work product, which requires ongoing business, and consent is not easily arranged; in the area of insurance; and in the area of employee information when termination is involved. All to say these are very specific circumstances where we think there are very legitimate and reasonable grounds for businesses to work with and share information among themselves.

I know, Kelly, you have some further information on this.

Ms. Kelly Gillis (Associate Deputy Minister, Department of Industry): In certain circumstances, there are organizations called investigative bodies, such as a law society, where they have concerns regarding clients lists or privilege being breached. Right now, under PIPEDA, they can be prescribed in legislation, in the regulations as an organization that can share information between, perhaps, two law firms, to understand whether a breach actually has taken place.

What we're proposing in this particular amendment is to align with what other provinces have done to streamline the administrative burden by not prescribing the organization in legislation, by having a four-part test to make sure that it's only under limited circumstances, and it's not a fact-finding mission. There has to be evidence of something happening, and the information being requested has to be in line with the investigation that's happening, and there has to be proof that asking for consent would compromise the investigation in and of itself. So there are measures in place to make sure that there is appropriately focused...and there is nothing preventing an individual from asking for the information later on how it was being used, or making a complaint to the Privacy Commissioner about how their information is being used. The general oversight provisions still apply.

The Chair: Thank you, Ms. Gillis.

Mr. Warawa, you have five minutes.

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

Thank you, Minister, for being here.

I think it's very important that we protect the rights and the personal information of Canadian consumers. We realize, with regard to the digital economy and how it's evolved so dramatically over the last few years, that it's important that we address the concerns we hear from Canadians.

With respect, Chair, I hear from the NDP that we should maybe amend what has come to us from the Senate.

Minister, if we were to delay and amend, would Bill S-4 then have to go back to the Senate to get passed? My concern is that this is needed, Canadians want this, and a vast majority of Canadians want this passed, and if we amend it, what's the chance of it passing in this Parliament? It's needed.

Hon. James Moore: Well, to answer the political question that I guess in part came from Ms. Nash, as a committee you can propose amendments and consider them, as with other legislation that we've brought forward, like the Copyright Modernization Act, and so on. You will vote on them and consider them, and they will be considered by the House at report stage when the bill comes back.

There's a procedural issue, of course, in that if the bill is amended it does go back to the Senate for reconsideration of the bill, because the process is reversed. But I certainly wouldn't advocate taking away from members of Parliament their right to deliberate over legislation and offer thoughtful amendment if it strengthened the bill.

To Ms. Nash's point, if members of this committee have amendments, if any member of this committee has suggestions on how the legislation might be improved, we can certainly do all we can to provide this committee with the necessary background information to understand its implications for the bill, and whether or not it would in fact strengthen it.

● (1155)

Mr. Mark Warawa: Thank you, Minister.

Chair, we will be discussing this in great detail. We'll be calling a number of witnesses. The reality is that in our calendar we have about 15 meetings in the rest of this Parliament. If it's not passed, forwarded to the House and then passed, this will not be going ahead in this Parliament. I believe it's needed. I believe we've heard—and the Senate heard—that this reaches the balance.

Minister, just to reconfirm, there is a review built into Bill S-4. This will be reviewed in five years to see if it's effective and if there are any problems with it. Is that correct?

Hon. James Moore: It can be reviewed at any time. This committee can choose its own business. You can review it the day after, if you like. The committee can do whatever it wants. But as my deputy points out, this is the third time we've taken a run at this legislation and updating PIPEDA, so there is some urgency.

I was in opposition for two terms and I understand the nature of chastising governments for reasons real and imagined. That's fine, but one of the reasons we took the approach, why it is Bill S-4, and why we tabled it in the Senate first, is that this committee had a very full agenda. Parliament itself had a very full agenda, with a number of high-profile and complex pieces of legislation through the fall session of Parliament, and we wanted to get going on this. We wanted to get forward traction.

Of course, our legislative process requires it to have the support and consent of both houses of our bicameral legislature. We wanted to get it passed and moving forward, keeping in mind that we do have a campaign coming up this fall and House time is precious and limited. We reversed the process for that reason: because we do want this legislation to get passed and we do want it to go forward.

We see it as essential for a number of reasons, including taking full advantage of the digital economy and protecting Canadians online. There is I think a growing anxiety and an expectation amongst Canadians that the government do all it can in order to protect the privacy of Canadians online, not only in terms of the Privacy Act and citizen engagement with the Government of Canada in ensuring that their privacy is protected when they provide their information to the government, but also when they are doing so in the private sector.

It has now passed the Senate after consideration and deliberation, and there are a number of amendments that were debated at committee. This committee of course can fill its schedule and consider this legislation as it wishes, but it certainly is my desire that the bill move forward and be adopted so that we can protect Canadians and give Canadians the confidence they deserve.

The Chair: Thank you, Minister.

Ms. Nash, you have two minutes, from the calculation of what is left after the last question.

Ms. Peggy Nash: Thank you.

Would you like to...?

[*Translation*]

Ms. Annick Papillon (Québec, NDP): Yes, I'm going to continue.

Bill S-4 would give the Privacy Commissioner additional powers to enter into compliance agreements with organizations. In light of the fact that the date of the budget has been postponed numerous times—it won't be before April—has the government committed additional financial and human resources to the commissioner so that he can fulfill his new functions?

You have been in power for nearly 10 years and you are preparing a new budget. Can you assure us that the commissioner will have sufficient financial and human resources to do the job properly?

Hon. James Moore: That's a good question.

Yes, we believe that the commissioner and his office have the resources they need to implement the bill effectively and reasonably.

Ms. Annick Papillon: Although we don't know what the budget will contain, you are sure that you have set aside the resources necessary for the commissioner to do the work properly. Is that what you are pledging, minister?

Hon. James Moore: Yes, we believe the commissioner has the resources necessary. If more resources are needed, we'll have to make some changes. The government can always make that decision. After conducting consultations, however, I can tell you that we are convinced the commissioner has the resources he needs.

● (1200)

[*English*]

The Chair: The last questioner is Mr. Daniel, for five minutes.

Mr. Joe Daniel (Don Valley East, CPC): Thank you, Chair, and thank you, Minister, for being here. It's great to see you.

Clearly one thing that is interesting is that the Internet does not have Canadian borders. It's obviously going right across the world; it's going everywhere else in a flash. Given that and the nature of data, you could have a very small company, run by one or two people, with terabytes of data that could be lost and moved upon.

Is a $100,000 penalty a reasonable penalty for a small company that would go bankrupt without it? They'd probably start again the next day, but....

Hon. James Moore: We think the penalties are aggressive, and they are per breach—it's not a macro figure. In the violent crime legislation that we put forward, this is not a concurrent fine; it would be consecutive. It other words, this would be per breach, per violation.

Mr. Joe Daniel: Excellent.

We have so much trade going on with companies that actually don't reside here, and I think you alluded to that earlier. But if their data is being housed out of country and they are working with Canadians, and if there is a breach of Canadian data and they have no footprint in Canada, how do we deal with that?

Hon. James Moore: As I said, this is about protecting the rights of Canadians, and if Canadians' rights have been violated, the commissioner is empowered to pursue those penalties and those investigations. It's about the rights of a Canadian citizen; it's not necessarily about the physical aspect. It's about those who are doing business in Canada interacting with Canadians through ISPs within Canada. It's about protecting Canadians.

Mr. Joe Daniel: Very good.

This seems to be very functional and well-written legislation. I think it is going to be very effective when we put it in place, so I agree with my colleagues that we should move forward with it with speed.

This is probably just a side issue. Have we have considered anything about legislating on the software and hardware that allow some of these breaches to occur? We've seen that Microsoft, for example, when it brought out its spreadsheet, had a whole flight simulator embedded in the software just to push the hardware out. There are surely things that we can do on that, and we can maybe legislate some of it.

Have you considered that, or has your department considered it?

Hon. James Moore: It sounds to me less of a privacy issue than a competition issue. But yes, there are always those accusations about some firm's new operating system or new software being bloated in order to drive up the demand and requirement for greater hardware. It's a well-told story and well understood.

I would say that, if you or anybody has concerns about that kind of anti-consumer behaviour, we have a competition commissioner who can certainly look at them.

Mr. Joe Daniel: I think there are hardware solutions that would prevent undue access, and similar software solutions as well, but that is just a comment.

Hon. James Moore: The one thing I would say is that since the mass saturation of personal computers, and now, with the increasing saturation of smartphones, people are spending. It used to be that you would spend $2,000 for a laptop and $200 for a mobile phone. Well, now you're spending $1,000 for a mobile phone and $500 for a laptop; and they're everywhere. We are all obsessed with the technological facts of our lives.

The consumer is far more educated. Some of the games that have been played in the past on the consumer side, such as the software/hardware dog-chasing-its-tail-in-order-to-drive-money-out-of-the-consumers'-wallets which we've just described, I don't think people could get away with today. People are more informed and have better understanding than ever before.

We're all exposed. We know what data plans are on the wireless side. We know what behaviour drives up our costs on the wireless side. People are getting more and more educated, and with information and knowledge comes power. With the power of an informed consumer come reacting market forces. With reacting market forces comes greater innovation. It's a good thing.

Mr. Joe Daniel: Well, thank you very much, Minister, and I think this is a wonderful bill. I think we should continue to press forward with it. It will be in the interest of all Canadians, including those in my riding of Don Valley East, and I'm hoping that we can get this through fairly quickly.

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

Thank you very much, Minister, for indulging a couple of minutes of overtime. We're going to pause for a couple of minutes while the minister leaves and while his officials get set up for the second hour.

● (1200)

(Pause)

● (1210)

The Chair: Colleagues, we're back in session.

We have a second hour, and Mr. Knubley has some opening remarks.

Mr. Knubley, please go right ahead.

Mr. John Knubley: Mr. Chair, I'll be very short.

I want to talk about two things. One is the basic objectives of the act, and the Minister referred to them. I also want to talk about some of the principles and objectives in terms of the design of the bill, which I think are important to understanding why the bill is the way it is.

[*Translation*]

Bill S-4 makes four important changes.

[*English*]

First, it requires companies to tell Canadians if their personal information has been lost or stolen, and they've been put at risk as a result.

Second, in the area of consent, it clarifies that actions taken to obtain consent must be appropriate to the target audience. We heard earlier about the particularly vulnerable group of children. In the area of consent it modifies the very limited circumstances—and we would want to stress, very limited—when personal information may be shared without consent in order to balance against other important public policy objectives, for example, if a bank or financial adviser suspects that one of the clients is a victim of financial abuse.

Third, Bill S-4 gives the Privacy Commissioner a range of new tools and greater flexibility to enforce the act.

Fourth, it take steps to reduce the burden on businesses and to allow them to use this information in relation to their ongoing work and due diligence relating to various business transactions.

On the design side—and this is what I think is probably most important as an administrator to bring to your attention—it is really two concepts. I think this came up in the earlier discussion. One is the issue of balance and the other is the issue of principles. This is a bill based on principles.

As we make amendments and look to the future we want to maintain a concept of balance and build upon a principle-based approach that has made PIPEDA successful. These principles are set out in the annex to the original act and include important concepts such as accountability, consent, accuracy, safeguards, and openness.

In light of some of the earlier questions I would stress that openness is a principle that we constantly look to and applies, for example, in the question of the use of information between businesses. Of course it is all about ensuring that citizens have the right to know.

In terms of balance, I'll make a couple of quick points. Ensuring Canadians have the information they need so they can take action to protect their privacy is a priority. Equipping the Privacy Commissioner with the information and tools needed to protect Canadians and increase compliance is a priority. Providing clear rules and a minimal administrative burden on the private sector is a priority. These are not priorities that always mesh and the question of balance comes into play.

In conclusion I want to say that while every country takes a unique approach to addressing privacy—the United States, for example, has a more regulatory-driven approach and the European Union a much more proscriptive approach—we think we have a world-leading approach to the administration of privacy here in Canada and that's reflected in these amendments. We hope to continue to be a leader internationally in this regard.

● (1215)

Thank you, Mr. Chair.

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

Colleagues, there's a committee coming in here after us. I know that because I'm on that committee. We have to do some business at the end so our rounds will be four minutes now per questioner in order to be able to finish on time and get the business done that we need to do and to be able to clear the room.

Mr. Lake, for four minutes, please.

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

I want to say I have had the benefit, being the parliamentary secretary, of having had briefings with you. Thank you for that. I expect this hour will show us how you're able to consolidate some fairly complex information, translate it, and help us to understand it in a short period of time. That is really a testament to the expertise that you have.

As Privacy 101, maybe you could start off with a quick explanation of the difference between PIPEDA and the Privacy Act.

Mr. John Knubley: I'll start and then ask my colleagues to help me out.

In brief, PIPEDA and the Privacy Act are quite different. PIPEDA applies to the private sector and its collection, use, and disclosure of personal information in the context of commercial activity. From a federal government perspective, that means specifically that the trade and commerce power is being applied as well. It applies to federally regulated industries, specifically, for example, to banks and telecom companies. The Privacy Act applies to federal governments and agencies and their handling of personal information.

These are quite different, and quite different in the sense of how the bills are conceived. PIPEDA is based on the concept of consent, generally requiring that an organization have the consent of the individual to collect, use, and disclose their personal information and based on the application of those principles that you'll find in the act. The Privacy Act is not based on consent, but instead is very prescriptive as to when and how federal institutions may collect information. No personal information, for example, shall be collected by a government institution unless it relates directly to an operating program or activity of the institution.

I'll conclude by saying that in the area of digital privacy, we feel that you need these principles and a balanced approach in order to take into account the changing technology. A balanced approach gives you the flexibility to still apply the rules, even though the hardware and the software are constantly changing, for example.

Hon. Mike Lake: For those who may be following these hearings over the next several weeks, something that might be helpful as well is to understand how the federal and provincial jurisdictions deal with privacy differently, because it seems to me that the provinces each have their own legislation similar to PIPEDA.

Why would there be a need to have legislation at both levels?

Mr. John Knubley: I'll let Chris elaborate, but the short answer is that we apply to federally regulated industries and they apply to provincially regulated industries.

Mr. Chris Padfield: That's right, and not every province has privacy legislation in place. PIPEDA basically blankets the whole of the country. In those locations that have moved forward with their own privacy legislation—Quebec, B.C., and Alberta—they have what is called “substantially similar designation” under our legislation, so we recognize that in those three jurisdictions, for privacy issues contained within the province those pieces of legislation take precedence.

You can see situations in which privacy issues cross borders, and then you see both the Privacy Commissioner federally and the provincial privacy commissioner working together to address issues.

The provincial powers are different from the federal powers. With the trade and commerce powers, we're restricted federally to issues that happen within trade and commerce activities, whereas provincially they break down into deeper, more regular activities of individual Canadians, rather than just those in the context of the commercial activities.

● (1220)

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

Now we go on to Ms. Papillon.

[*Translation*]

You may go ahead for four minutes.

Ms. Annick Papillon: By referring the bill to a committee before second reading, the government opted to take a different route.

Could you please tell me why the government referred the bill at that stage, before second reading? Could it be that the bill, in its current form, might be deemed unacceptable given its deficiencies, making it necessary to follow such a process?

Moving the bill through all these stages has prolonged the process. I'd like you to tell me why the government decided to proceed that way.

[*English*]

Mr. John Knubley: Mr. Chair, these are decisions of the government and not decisions of officials, so I don't think it would be appropriate for me to comment on this.

The Chair: Thank you, Mr. Knubley.

Go ahead, Ms. Papillon.

[*Translation*]

Ms. Annick Papillon: Bill S-4 would require organizations in the private sector to report any loss or breach of personal information. But the criterion on which that mandatory reporting is based is subjective. In fact, the bill allows organizations to determine, themselves, if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.

Why didn't the government choose a more objective criterion as the basis for that determination, such as the one proposed in Bill C-475, An Act to amend the Personal Information Protection and Electronic Documents Act (order-making power), which was introduced by my colleague?

[*English*]

Mr. John Knubley: Again, I think the model that we have here is to ensure that the Privacy Commissioner

[*Translation*]

has adequate powers precisely to examine the problems. Given the current context, the bill enables Canadians to ask organizations exactly what happened to their information.

Ms. Annick Papillon: But why didn't you use a more objective criterion, such as the one in Bill C-475, which was introduced in 2012?

Since the government's bill is modelled after Bill C-475, why wasn't a more objective criterion used?

Mr. John Knubley: As I just said, I believe the bill is based on principles. It's always important to find the right balance. What the bill does is make it unnecessary to impose conditions outright.

[*English*]

I'll ask Chris to explain further.

Mr. Chris Padfield: If I understand the question on the data breach provisions correctly, with regard to whether it's the private sector making the risk assessment versus the data breaches going specifically to the commissioner and having the commissioner review all the data breaches, in the approach that has been put forward in Bill S-4, the outcomes end up being the same.

When an individual company does an assessment of the risk of the data breach and whether there's going to be harm to the individual, they go through the procedure for figuring out whether they have the risk. Once they've identified that there's going to be a risk of harm, they identify both the individual and the Privacy Commissioner. At the same time, when they've done that assessment and they've reviewed the data breach, if they've found that there is no risk of harm, they're required to maintain a record on those and the commissioner can ask for those records at any time. They could ask the individual company to report all of those records to them at any time. So the commissioner has access to the same types of information and can review all those at any time.

The end result is the same. The commissioner has access to any and all data breach records at any time he wants, whether there's a real risk of significant harm or otherwise.

The Chair: Thank you, Mr. Padfield, that's all the time we have.

Now we have Mr. Carmichael for four minutes.

Mr. John Carmichael: Thank you, Mr. Chair.

Mr. Knubley, I'd like to go back to a question my colleague Ms. Gallant asked the minister about in the first round and that is with regard to red tape reduction.

In your opening remarks you talked about the concept of balance and about what's made PIPEDA successful over the years. Principles set out in the annex included important concepts such as accountability, consent, accuracy, safeguards, and openness to just name a few. In your opening statement, you talked about the five significant changes to the act and in number five, you talked about reducing the burden to business and a number of elements that are listed there.

I wonder if you could just elaborate on how this bill is going to ensure that we don't increase but rather reduce red tape, because as you know that has been a focus of our government for the last several years up to and including its own act, the red tape reduction act, which is a very important part of what we believe is important to the economy. I wonder if you could just elaborate on that for us, sir.

● (1225)

Mr. John Knubley: These amendments were done very much in the context of the 2007 five-year review. I think there was an assessment at that time around the issues of the burden to businesses with respect to PIPEDA.

I think there are five very specific, and I would add limited, amendments in this area to improve and streamline the obligations of business. One is related to business contact information; we're talking here of an email address or a fax address. This would exclude all types of business contact information, provided this information is only being used to communicate with the individual with respect to their employment, business, or profession.

Of business transactions, the most concrete example is mergers and acquisitions, and if two businesses are going through both a merger and an acquisition then it's deemed appropriate to share information without consent.

Mr. John Carmichael: Was that previously restricted?

Mr. John Knubley: Correct.

Work product is a concept that I think is in the bill. The issue is, can the businesses carry on their activity without sharing the work product? An example might be an inspector who has signed a bill of activity and he's put his name at the bottom. Can the businesses share the actual bill between the two companies?

Processing of insurance claims and employee information, I think typically relates to termination. Chris, help me out on the explanation of these very limited circumstances.

Mr. Chris Padfield: It's very specific and very common sense. A lot of them come from that second Parliamentary review. Because in PIPEDA consent lies across everything as a principle, there are some very specific circumstances.

I think the business transaction is a great one. When companies are looking to merge, they don't want to have to go through and get consent from every customer on each side of the border, which is the way PIPEDA kind of reads now. You have to go back to each person or client and get their individual consent that you can share their information with the other company when you go through that transaction. It just doesn't make sense.

Mr. John Carmichael: So it's going to simplify that process.

Mr. Chris Padfield: It simplifies that process. It covers and protects the key people involved because it makes sure that there are contractual obligations. If the transaction doesn't happen, the company that receives information has to destroy the information. It's a very clear, common-sense approach to business transactions.

Even on the data breach side, we've streamlined the approach of data breach to minimize the number of tests and how the reporting is done to make sure that it's only meaningful reporting for Canadians. It minimizes the burden on industry in that reporting system.

The Chair: Thank you.

[*Translation*]

Mr. Dubourg, you have four minutes.

Mr. Emmanuel Dubourg: Thank you, Mr. Chair.

I'd like to pick up on the part of Bill S-4 that concerns the transfer of information between the organizations.

I'd like to first say I think it's very commendable to have a bill that seeks to protect the elderly and young people when they are sharing information online. But I am troubled by the total lack of oversight when it comes to public institutions sharing information among one another, including law enforcement agencies. The information is being shared without the individual's consent or any monitoring. There is an absence of any civil liability in that regard.

Don't you think the bill should be amended to address that? The Privacy Commissioner is involved, especially when it's a matter of security, but in other cases, as I just pointed out, the information is being shared without any oversight.

● (1230)

Mr. John Knubley: That's a very good question. We'll explain to you how that can be addressed.

Generally, I think the four following criteria are now applied.

Is it an issue that concerns the private sector?

Is there really a risk of fraud or of a problem arising between the companies and does it affect Canadians?

Also applicable is the test of reasonableness.

So it's not fair to say that there are no such provisions to that effect.

I will ask Christopher to explain.

[*English*]

Mr. Chris Padfield: I think the deputy covered it fairly well. The other thing to remember here and at all times is that the underlying principle of PIPEDA is openness. In any circumstance, if there are any Canadians ever concerned with how their information is being used by a private sector organization, this overlies everything there is in this provision.

Canadians have to be given full access to their information. They have to be able to assess its accuracy and corrections have to be made, so that if Canadians are ever concerned at any time, it's the ultimate oversight.

PIPEDA is designed to give Canadians that authority for themselves so they can go and ask any organization that has their information to see what information they have and to share its accuracy. If they don't get that information, they can go to the Privacy Commissioner, make a complaint, and the commissioner can go forward.

[*Translation*]

Mr. Emmanuel Dubourg: Thank you for the explanation.

You said that people could always file a complaint with the commissioner, but one of the underlying principles of the bill is to ensure that Canadians have the information they need so they can take the necessary steps to protect their privacy.

If organizations are sharing information about an individual without their consent, how can that person take steps to protect themselves? First and foremost, if I find out that my personal information has been shared between organizations at whatever level and that my information may be at risk, I would be the first to want to take steps to protect myself. But all of this is going on without my consent, without the consent of the person concerned.

Don't you think that—

[*English*]

The Chair: We're over time, Monsieur Dubourg.

[*Translation*]

Mr. John Knubley: Basically, the act and amendments impose obligations of that nature on organizations. Bill S-4 sets out new obligations.

[*English*]

The Chair: Madam Gallant, for four minutes, please.

Mrs. Cheryl Gallant: Thank you, Mr. Chair.

For you, Mr. Knubley, we had Peggy Nash asking a question and she cited a number of clauses from legislation as to when the information on customers would be shared. What it sounded like was that during an online transaction the reference may have been made to PayPal, iTax, or credit card companies allowing them to share, for that transaction only, the information.

While you gave a very succinct answer on how it comes into line with provincial legislation, I'm wondering if you could tell me if, for the purpose of purchasing online, that's why those references are made.

● (1235)

Mr. Chris Padfield: For those specific provisions, currently under PIPEDA there's a regime called the investigative body regime. It lists a number of entities that are allowed to do these activities now. The range of entities that are there are, for example, the bank crime prevention organization that works for the bank association. They share information back and forth among banks around people who have been robbing ATMs. They have videos at ATMs. They use and share that information without the thieves' consent so they can identify and do an investigation into the crimes. I've visited them. They share information across the country from different banks on people who are stealing from ATMs or robbing right inside the location. It's that kind of sharing we're talking about in that context.

Under the current investigative body regime there are those kinds of sector organizations. Then there are professional associations, such as professional engineers associations, colleges of physicians and surgeons, and the Law Society of Upper Canada, that do investigations into their own members in assuring that their own members are following the code of conduct for their organizations.

You have a third grouping such as forensic auditors who do that kind of activity on behalf of somebody else.

They share information without consent in the course of investigations. These investigations are generally for other public policy purposes in protecting Canadians from crimes, as in the bank example. That kind of information gets flowed back and forth.

What Parliament recommended in the first review of the act was to take an approach of regulating the activity rather than regulating the specific entities, which is the approach that B.C. and Alberta have taken. Rather than having the prescribed list of organizations that has to be updated—if you change your name, you have to go through regulation to have your name changed in the regulation—they said regulate the type of activities rather than regulate the individual entities and put them all on a list in the back.

That's what S-4 has done. It's taken that investigative bodies regime and split it into these two other sections to go and regulate the type of activity rather than the bodies themselves. That's what Parliament recommended and that's what B.C. and Alberta do now.

Mrs. Cheryl Gallant: Okay, and of course no legislation happens in isolation and we currently have the anti-terrorism legislation before us. With that proposed legislation and PIPEDA, confirm for me that should information be required from a company there would be a warrant required for that purpose. Or is that the automatic sharing you're referring to as well?

Mr. Chris Padfield: They are completely separate pieces and not related. The anti-terror law is about exchange of information within government. This is about private sector privacy rules. They're quite separate pieces.

Mrs. Cheryl Gallant: To answer my question would a warrant—

Mr. John Knubley: To answer your question I think the first step is always to ask if there is a warrant. The next step is to ask if there are any limited areas where consent is not required, and there are some very specific areas where that applies. That's the way the digital privacy act works.

I should be clear that this law does not apply to the police. This is a law that applies to the exchange of information from businesses to citizens.

The Chair: Thank you very much, Mr. Knubley, Madam Gallant.

Now to Ms. Borg for four minutes, please.

[*Translation*]

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

I'd like to come back to the last line of questioning.

I realize that exceptions can be warranted, as you explained, and that's okay. But it opens the door to abuse. We've seen it repeatedly. PIPEDA currently sets out exceptions. Government agencies have made at least 1.2 million requests for information to Internet service providers. So the provisions in PIPEDA have already led to abuses.

And now we are opening the door to more potential abuse. I realize a specific intention is underlying these amendments, but it's very problematic when you open the door up to abuse. I think Canadians want a system that doesn't lend itself to abuse.

Do you think the bill gives them that assurance?

Mr. John Knubley: Yes, that assurance is there. I will explain again. The act already sets out exceptions. Amendments are being made, but the exceptions are already there.

● (1240)

Ms. Charmaine Borg: My other question has to do with the mandatory breach reporting mechanism.

In your opening statement, you said you wanted to provide clear rules and create a minimal administrative burden on the private sector. I think everyone supports that. But the discretion to decide whether reporting poses significant harm to the individual is left to the organizations subject to PIPEDA, and that concerns me.

I know there are a number of big companies. We tend to think of the Internet giants, which have privacy protection officers, who are tasked with ensuring respect for people's privacy. The problem is that 98% of companies are small or medium-sized. How are you going to help them and support them? Will small and medium-sized businesses be given tools to guide them as they try to figure out whether a breach poses significant harm?

[*English*]

Mr. Chris Padfield: As we go through this, there are lots of things that have to be established through regulation. We're quite conscious of the fact that these data breach provisions apply, from the local dry cleaner down the street all the way up to a big bank or a telecommunications provider. We're looking for the most simplistic ways we can have in terms of reporting, in giving out clear guidance. We'll work with the Privacy Commissioner's office once the provisions are in place to come up with really clear, straightforward guidance for small companies. We are conscious of the fact that this does apply all the way from the mom-and-pop shop up to the major multinational corporations that are better prepared for these kinds of things.

[*Translation*]

Ms. Charmaine Borg: Thank you.

Do I have any time left?

[*English*]

The Chair: You have 20 seconds.

[*Translation*]

Ms. Charmaine Borg: Thank you very much.

[*English*]

The Chair: So actually, there's going to be outreach. You're saying there will be some outreach in that regard.

Mr. Chris Padfield: To bring the data breach provisions into force we're going to have to pass regulations, so we'll need to consult on the regulations and go through that. Then after that's done it's the role of the Privacy Commissioner to help provide guidance to companies about how to comply in these areas.

The Chair: Thank you.

Mr. Warawa for four minutes, please.

Mr. Mark Warawa: Thank you, Chair.

Under the data breach notifications, a business that's been hacked will be required to let their customers know that there has been this breach and they could be at risk. What's the timeframe they have to notify their customers? Who determines what is a reasonable length of time?

Mr. Chris Padfield: It's specified in the law as "as soon as feasible". For us that means once you've closed the breach, you're not at risk by informing folks. If the breach is ongoing, by going around informing people it could be further exasperated, so once you've clearly identified the breach and you're able to contain it and move forward with it.

It's meant to be as soon as feasible, so without any undue delay. The exact time's not specified because each breach is different. There could be quite a few different elements.

In terms of determining that risk assessment, we haven't prescribed, and in general PIPEDA doesn't prescribe. It isn't very prescriptive in terms of providing these kinds of things. It provides a general sense.

Mr. John Knubley: I can maybe just add, though, that in terms of the offences that are under the act, there are three new ones related to data breach. There's a real demand for compliance in this respect. New offences are related to failing to report the data breach to the commissioner as required, failing to notify an individual of the data breach as required, and failing to maintain the records. These are actually offences now, so there is a lot of incentive for firms to do what is required as soon as possible.

Mr. Mark Warawa: A fine of up to $100,000 per individual is substantial and could destroy a company.

Who determines the appropriate fine, and what do we have for an appeal?

Mr. John Knubley: The Federal Court would determine the fine based on a number of...how frequently this has occurred. That is, like you said, an "up to" fine.

Mr. Mark Warawa: There is no minimum.

Mr. Chris Padfield: No.

● (1245)

Mr. John Knubley: I think specifically it is the Director of Public Prosecution who enforces it.

Mr. Mark Warawa: So discretion is left with the courts to set a maximum fine.

On seniors' issues, the minister shared the concern that the government has on senior abuse, which is very warranted, and I agree with him. Senior abuse, though, can happen in many different forms, not necessarily within family. It can be unscrupulous business; it could be even through mail theft, or a phone scam—so many different ways.

I'm from the Vancouver area, and mail theft is a huge problem. Canada Post has changed their mailboxes to make them much more secure.

What responsibility do financial institutions have if they have mailed a new credit card to a senior and that card has been activated in fraud? Does the senior have any responsibility?

Mr. John Knubley: I'll get Chris to help me out again, but I think the particular case you're raising is moving into the Criminal Code, as opposed to being within the purview of PIPEDA.

Having said that, under PIPEDA currently, a bank cannot contact anyone. The amendments we're providing for will allow them to do this within the specific context of financial abuse relating to the banking transactions.

Mr. Chris Padfield: When you're getting into credit card fraud and identity theft, that falls to the Criminal Code. Like the deputy said, there's a very specific amendment here.

If you're a teller in a rural bank and you have a regular elderly customer coming in with somebody and you clearly see the customer handing off cash to them, right now PIPEDA constrains you from being able to call anybody in the family to say that you've noticed their mother coming in lately and people have been taking her money, or she's been giving money to somebody you don't know and you want to make sure they're aware of that. They can't do that now under PIPEDA. PIPEDA restricts them from being able to give out that personal information. This takes that away.

The Chair: Mr. Padfield, thank you very much.

Now, on to Ms. Nash for four minutes.

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

Again, I want to emphasize that I think there are many provisions in this bill that Canadians are looking for and feel are long overdue, and they are happy to see. I think it's unfortunate that there are some other provisions in this bill that are creating a lot of concern. Canadians are very concerned about their digital privacy, which is why this bill is being brought in. Yet, the area of warrantless disclosure is one that has been highlighted. It was highlighted at the Senate committee. While there may be absolutely legitimate areas where it makes sense to have warrantless disclosure, it's the lack of oversight that's troubling here.

I just want to cite quickly a couple of pieces of testimony on Bill S-4. First of all, Peter Murphy, who is a partner at a Canadian law firm, Gowling Lafleur Henderson, says again there are some welcome changes in Bill S-4. But he also goes on to comment in particular on the provisions allowing for disclosure of personal information without consent between organizations in support of investigations and breaches of law agreements or fraud cases of financial abuse, and I'm quoting:

> This change would seem to permit fishing expeditions by companies seeking to sue individuals. For example, copyright holders would have grounds to freely obtain lists of internet addresses of individuals to find and sue internet downloaders. This seems to be a significant invasion of privacy if reasonable controls are not added to the proposed wording.

Michael Geist, who is a law professor here at the University of Ottawa, is an expert on digital matters, and he says:

> Unpack the legalese and you find that organizations will be permitted to disclose personal information without consent (and without a court order) to any organization that is investigating a contractual breach or possible violation of any law. This applies both past breaches or violations as well as potential future violations. Moreover, the disclosure occurs in secret without the knowledge of the affected person (who therefore cannot challenge the disclosure since they are not aware it is happening).

So, my question is, why is there not greater accountability, greater oversight, to ensure that this provision, if you do believe it is necessary, is not abused?

● (1250)

Mr. John Knubley: The approach that we're taking here, as we've indicated, is that in the areas that we're talking about they are extremely limited and very specific. We referred earlier to the four tests. Let me talk a little more about those because I think they're relevant to the question you just raised, which is, specifically, that the sharing of information between companies cannot occur unless there truly is evidence of a real investigation, say, for example, with respect to fraud.

Also, there has to be demonstration, and it's consistent with these four tests, that if the information was not shared, the investigation that is under way would be compromised. In other words, the seeking of consent would actually compromise the investigation.

Again, we as administrators consider the changes to be in line with what other provinces are doing, and they're in line with the existing act because these provisions already exist within the act.

The Chair: We'll move now to Mr. Daniel for four minutes.

Mr. Joe Daniel: Thank you, Chair.

Thank you, folks, once again.

My questions are always a bit skewed, I know, so we'll try to work with that. This bill has been focused very specifically on business-to-business, business transactions, etc., but there are tons of NGOs and tons of charitable organizations that have a lot of personal information. Does this bill take that into account as well? Can we do anything about that? The example is, I'm a volunteer and I go to, I don't know, the Heart and Stroke Foundation, and I take a look at all of their donor lists, and take a USB and copy it all, and use it for my own purposes or sell it to somebody.

Mr. John Knubley: The short answer is that the bill only applies to commercial activities, so if an NGO is involved in commercial work, then this bill applies.

Mr. Chris Padfield: If the NGO were selling products or something like that and there was a commercial aspect to it, it would apply. Generally if it's outside the commercial frame, PIPEDA does not apply.

If it's in a provincial jurisdiction, it may apply.

Mr. Joe Daniel: Generally, they're not selling anything per se. They're collecting money for some worthy cause, right? But there is personal information on many people in there.

Mr. John Knubley: PIPEDA is but one act that is relevant to these privacy issues. We've talked about the Privacy Act, and it's quite different. There's the Criminal Code. That would be another important element of it.

Mr. Chris Padfield: Privacy falls across so many pieces of legislation. Even the cyberbullying act has very specific pieces of privacy legislation there identifying specific uses or not for intimate images. That's another example of the other pieces of legislation that touch on privacy issues.

Mr. Joe Daniel: Say I've stolen a whole bunch of information and I'm now going to start reselling it, for whatever reason, whether it's pictures or anything else like that. Is there legislation that would criminalize me personally for doing that? I presume so. It may not be in this legislation.

Mr. Chris Padfield: Yes, with any possession or creation of identity documents, as soon as you're getting into that kind of criminal activity, you're getting into identity theft issues that are covered by the Criminal Code.

The Chair: Colleagues, we're very close to our time. I think by the time we went in camera to do the business, it would be difficult to deal with it.

Madame Borg.

[*Translation*]

Ms. Charmaine Borg: Mr. Chair, I have a question or, rather, a request.

Further to all of the questions and answers we've heard today, I think it would be helpful to all the committee members if the analysts could prepare something for us on the Spencer decision. I don't know if the rest of the committee would like that, but I think it would be helpful.

● (1255)

[*English*]

The Chair: You can request that yourself, Madame, and we will make sure that's available.

[*Translation*]

Ms. Charmaine Borg: I think everyone would benefit from receiving it.

[*English*]

The Chair: We'll make sure that a brief on this is available for the members who desire it.

All right, colleagues, the small piece of business I had will be okay until the next meeting.

The meeting is adjourned.