HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Industry, Science and Technology

INDU • NUMBER 040 • 2nd SESSION • 41st PARLIAMENT

EVIDENCE

Tuesday, April 21, 2015

Chair

Mr. David Sweet

Standing Committee on Industry, Science and Technology

Tuesday, April 21, 2015

● (1105)

[*English*]

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

[*Translation*]

Good morning, everyone.

[*English*]

Welcome to the 40th meeting of the Standing Committee on Industry, Science and Technology. Today we're considering Bill S-4, an act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another act.

We are pleased to have three experts here, officials from the Department of Industry. Lawrence Hanson is the assistant deputy minister for science and innovation. Christopher Padfield is the director general of the digital policy branch, and John Clare is the director of the privacy and data protection policy directorate.

Thank you very much for joining us, gentlemen, and for being here for questions.

Colleagues, we have, as you can see piled in front of you, quite a number of proposed amendments to the bill. I was saying to my fine officials beside me that a chair never does this enough to get really slick at it, so we'll proceed, with your patience, through the bill. The officials have kindly batched the amendments together.

Unless I have some specific instruction from you, colleagues, on how to proceed, I'll just begin with the first clauses that have no amendments, then we'll move to the clauses that have amendments, and proceed in that way.

Is that fine for everyone?

An hon. member: Yes.

The Chair: It appears to be that way. You're always very talkative this early in the morning.

Shall clauses 2 to 5 inclusive carry? There are no amendments proposed for them.

(Clauses 2 to 5 inclusive agreed to)

(On clause 6)

The Chair: On clause 6 there are a number of proposed amendments, approximately 20.

I should tell you that if amendment NDP-1 is adopted, all the rest cannot be proceeded with, because of course they cannot amend the same line.

We're considering amendment NDP-1 now, which is actually right at the top of our pile here. It's page 1 of the documents you have.

Madam Borg.

[*Translation*]

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

Following the testimony we have heard, and several revelations in the media, parliamentarians and society realized that, unfortunately, there are far too many cases where the exceptions in the PIPEDA are used in far too broad and vague a way. There is no transparency regarding the exceptions that permit the sharing of personal information without consent and without a warrant.

I think that today we have to broaden our study and not only examine Bill S-4 and PIPEDA. That is what we must do when we study a bill at second reading.

That said, I move that section 7 of PIPEDA be repealed, so as to correct the flaws in this law that allow for the sharing of personal information without consent and without warrants.

[*English*]

The Chair: Mr. Lake.

Hon. Mike Lake (Edmonton—Mill Woods—Beaumont, CPC): If we could, I would just like to go to the officials to maybe get some feedback on the impact of this amendment.

Mr. John Clare (Director, Privacy and Data Protection Policy Directorate, Department of Industry): Thank you, Mr. Chair.

As was pointed out, the amendment would essentially repeal section 7 of PIPEDA, which sets out all the exceptions to the requirement to have consent to collect, use, or disclose personal information. This would remove every exception to consent set out in the bill and would mean that a company or an organization would require knowledge and consent every time it collected, used, or disclosed personal information in any context.

The exceptions that are there are set out for various reasons. In certain circumstances, it isn't practical to obtain consent if someone is injured, ill, or deceased, and sometimes obtaining consent would create conflict in law. For example, there's a provision in subsection 7(3) that allows disclosure without consent to comply with a warrant, subpoena, or other court order. This amendment would eliminate all of those exceptions.

Hon. Mike Lake: So even with a warrant...?

Mr. John Clare: An organization would be faced with either complying with the warrant and violating PIPEDA, or refusing to comply with a warrant to be in compliance, so it creates a conflict in law.

Hon. Mike Lake: This seems like a very broad removal here.

Are there other examples of how...? It seems to me there might even be other examples or even crazier situations whereby someone wouldn't be able to get consent.

Mr. John Clare: If you look at subsection 7(1), there is an exception to the requirement for consent for journalists or artists to collect personal information to use in a newspaper article, for example. So if a journalist were to interview someone about you as a member of Parliament, if the amendment were to be adopted, the journalist would require your consent to write an article that has a politician's name in it.

Hon. Mike Lake: That doesn't sound so bad.

Voices: Oh, oh!

So on budget day today, for example, if someone wanted to write an article about Joe Oliver, they would need his consent.

Mr. John Clare: That's correct.

Or if you were to look up information in the phone book, it's personal information. If you want to look up someone's name, you're collecting their personal information and then using it. Technically you require their consent.

Hon. Mike Lake: That's enough, I think.

The Chair: Ms. Sgro.

Hon. Judy Sgro (York West, Lib.): Before PIPEDA was in place what would have happened?

Mr. John Clare: There was no prohibition against the collection, use, or disclosure of personal information.

Remember that PIPEDA creates this general prohibition. It says that you can't collect, use, or disclose without consent, except in these circumstances. Section 7 sets out those circumstances whereby you can collect, use, or disclose without consent.

Hon. Judy Sgro: But prior to PIPEDA being in effect—

Mr. John Clare: People could collect, use, and disclose for any purpose, without consent.

The Chair: Is there any more discussion on NDP-1?

Colleagues, as I mentioned there are some 20-odd amendments here. We're simply talking about NDP-1 right now, and then we have probably closer to 25 that pertain to clause 6.

Are there any suggestions about how you would like me to proceed? I apologize; there are probably 45 amendments for clause 6, now that I see we have a double-sided sheet.

● (1110)

Hon. Mike Lake: I think there are 21 just for clause 6.

The Chair: Yes, Ms. Sgro.

Hon. Judy Sgro: Given the fact that all the amendments that have been put on the order paper are from opposition parties, and no amendments have been put forward by the government side, just being very practical for time.... I'm happy to spend the next four meetings going through all of them, but just to be clear on the timing, if the government intends to vote against all of the amendments, then I think we need to know that as we continue with our meeting. They have the majority so we're going to go through a very long process of amendments.

Hon. Mike Lake: What would be the impact of that?

Hon. Judy Sgro: If you vote against all these amendments, all 40 of these amendments are going to fail and the bill will go forward in its current condition.

Hon. Mike Lake: Do you want to move all the amendments together?

Hon. Judy Sgro: No, I'm just saying that I think we should have a discussion. You asked if there was any way we could deal with the timing of all these amendments. I'm just suggesting that if the government is going to vote against all of them, that is something we should have a discussion about because the next four meetings as we do all this will be a really futile waste of time.

I'm quite happy to do it. I just think we should know where the government is coming from and why they didn't move any amendments.

Hon. Mike Lake: I think it would be good to hear the arguments in favour. Keep in mind that many of the amendments are duplicates from Mr. Hyer and from Ms. May, so the half that are Ms. May's will not be moved because Mr. Hyer is going to move his.

I think it would make sense to group them, but I certainly want to hear about them and give opposition parties the chance to explain why they're moving the amendments they're moving. For situations where there are almost identical amendments moved by multiple members of the opposition, I think then certainly we could group them together and hopefully move fairly quickly through those. But I certainly think it would be best for us to make sure that we hear the arguments that opposition members have in favour of the amendments before we make decisions.

The Chair: All right.

Shall amendment NDP-1 carry?

Ms. Charmaine Borg: Do you want to vote on each one?

The Chair: Yes.

(Amendment negatived [See *Minutes of Proceedings*])

The Chair: We'll now go to amendment PV-2. I believe that is Mr. Hyer's.

Mr. Bruce Hyer (Thunder Bay—Superior North, GP): Thank you, Mr. Chair.

As you know, these three paragraphs in amendment deal with sharing information related to insurance claims. Our amendment is based on recommendations from the Privacy Commissioner.

Bill S-4 contains three separate provisions allowing an organization to collect, use, or disclose witness statements without consent at the request of the insurance industry. We have not been presented with any information or evidence demonstrating that the absence of these provisions has created any problem for the industry. We introduce these amendments in the hope of limiting the potential for fishing expeditions, to put it bluntly.

The Chair: Mr. Lake.

Hon. Mike Lake: Could we have a quick explanation from the witnesses on the impact of the amendment?

● (1115)

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

This issue was raised during the first statutory review of PIPEDA that was carried out in 2006-07. The recommendation of the committee at the time was that the government consult with stakeholders and the Privacy Commissioner to examine the issue of the use of personal information when it's contained in a witness statement for the purpose of processing an insurance claim.

There was a concern raised at the time and discussed during the consultations. If I witness an accident, say that I saw an individual recklessly driving through an intersection, and provide that witness statement to the police, there was concern in the insurance industry that the individual who drove recklessly through the intersection could refuse and not provide consent for the use of his or her personal information—the fact that they were at that place at that time—for the purpose of processing the insurance claim.

Based on the consultation, there was a pretty wide agreement among the stakeholders, including privacy advocates at the time, that you didn't want to create a situation whereby individuals can protect themselves from responsibility in an accident, essentially, by invoking their personal privacy and saying that the witness statement can't be used because it contains their personal information. The purpose of the amendment in Bill S-4 is to provide a very limited exception so that insurance companies can get access to witness statements that contain personal information, only for the purpose of processing the insurance claim.

The Chair: Is there any other debate? All in favour?

(Amendment negatived [See *Minutes of Proceedings*])

The Chair: Next is amendment Liberal-1.

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

I'll try to be brief and speak directly to the issue. The amendment I put forward would restrict the exception to circumstances where the employee is aware that the information is being collected and that the intended use of the peripherally collected information is consistent with the intent of the original work. As an example, notes created during a job interview by the interviewer would meet that definition.

The Chair: Mr. Lake.

Hon. Mike Lake: In the interests of time, maybe I will ask the officials about this.

It looks like we have six amendments, with a couple of duplicates from the Green Party, so maybe it's four amendments in total that deal with the work product sort of area. Maybe you could explain the impact of those amendments in one shot as opposed to my asking you about each individual amendment.

Mr. John Clare: Absolutely.

This group of amendments deals with the way PIPEDA is structured. There's always an exception to collection, an exception to use, and an exception to disclosure. This group of amendments deals with exceptions to the collection and use of personal information that is a product of someone's occupation, their work.

Together the proposed amendments limit the exception to say it would apply only to personal information that was created with the knowledge or consent of the individual, and only to personal information that was incidental to the work products, not the main focus.

It would create a requirement on an organization to first ensure that the personal information in question in the work product...that the individual is aware that they created it and that it is personal information that they put in the product.

The second part would qualify that the personal information has to be incidental. There are two definitions of "incidental" in the Oxford dictionary. One is that it means less important, secondary, or subsidiary. The other definition is that it's connected with, related to, or associated with something. There's some line you'd have to distinguish between when it is the main part of the work product and when it is incidental to the work product.

The Chair: Is there any discussion on that?

(Amendment negatived [See *Minutes of Proceedings*])

The Chair: Next would be amendment PV-4.

Mr. Bruce Hyer: Mr. Chair, in the interest of time you might want to lump together PV-4 and PV-5. I can make a brief—

● (1120)

The Chair: Those are both yours, Mr. Hyer?

Mr. Bruce Hyer: Yes, they are.

The Chair: Please, go ahead and speak to them.

Mr. Bruce Hyer: Mr. Chair, these amendments deal with work product exemptions. They're based on CBA recommendations regarding use at work. We can envision scenarios where the broad language of the proposed legislation could be abused.

Keystrokes on a computer, records of comings and goings, images on covert video surveillance are all personal information. If these provisions are retained, they should be restricted to personal information that the individual is contracted to produce, with the knowledge of that individual.

The Chair: Do you want to go to the officials, Mr. Lake?

Hon. Mike Lake: Are you sensing a trend?

The Chair: Please, could the officials comment on that?

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

The amendment is substantively the same as the Liberal amendment, so the analysis is the same. You have to have the knowledge and the consent of the individual in producing the information, and the personal information has to be incidental to the work product.

The Chair: All right. We're looking at PV-4 and PV-5.

(Amendments negatived [See *Minutes of Proceedings*])

The Chair: Thank you very much. Now we'll go to amendment Liberal-2.

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

Clearly, this is an area that many of us on this side have concerns with. The CBA, as well as others, flagged it as having potential problems. Clearly, a work product exemption to the definition of "personal information" is generally understood to encompass non-sensitive personal information incidentally created in the course of one's employment, which you referenced.

But it's that whole issue of consent that continues to be a problem. Again, my amendment is going to restrict the exception to circumstances where the employee is aware that the information is being collected and where the intended use of the information collected is consistent with the intent of the original work, such as during a job interview, and would meet that definition.

Again, it's that same issue. You must be aware of the fact that we all have concerns about it on this side. Do you not think there is some way we can clarify this particular issue to make it clear what kind of definition we're talking about?

The Chair: Mr. Clare.

Mr. John Clare: I think there are two ways in which the issues you're raising are addressed. The first is that part of PIPEDA, in section 5, provides this overarching requirement that any collection, use, and disclosure be reasonable in the circumstances. Notwithstanding whether you get someone's consent, notwithstanding whether an exception applies, a court or the Privacy Commissioner looking at a complaint under any of these exceptions would first determine whether the actions of the organization were reasonable.

That applies in a lot of situations in the workplace, for example with video surveillance. It may be reasonable to install video surveillance in the teller area of a bank, but it wouldn't be reasonable to install that surveillance in the bathroom. That's already been applied, and that reasonableness standard would apply to this exception as well.

The other point is that the use has to be consistent with the purpose for which the information was collected. The example that I use is that if I'm an employee of Industry Canada and my boss says, we want to put you in a video to talk about how great it is to work for the public service, and I agree to do that, they can turn around a year later and recut that video and still use my personal information, my image. They don't necessarily have to go back and get my consent, provided that the video they produced is consistent with the original purpose, which is to promote the public service. What they couldn't do is take that video and then, say, sell it to an advertiser to then use my image for offering products for training to public servants, or something like that, because that wouldn't be consistent with the purpose for which the information was originally collected.

● (1125)

The Chair: Madam Sgro.

Hon. Judy Sgro: Mr. Chair, what about the issue of monitoring computer keystrokes as a way of punishing an employee?

Mr. John Clare: To the extent that they're collecting personal information, if their use of that personal information they're collecting is consistent with the purpose for which it was collected.... Monitoring keystrokes is the same as looking at the document you've typed. If they're using the document for a purpose that's consistent with why it was originally created, then it would qualify for the exception. If they're using those keystrokes in some completely unconnected way, it's inconsistent with the original purpose, it wouldn't be permissible under the exception. If they were doing it in a manner that a court considered unreasonable, in other words it wasn't fair, it didn't demonstrate a use of good judgment, if it was patently unreasonable then the exception wouldn't apply either.

Hon. Judy Sgro: Thank you.

The Chair: Is there any other discussion?

(Amendment negatived [See *Minutes of Proceedings*])

The Chair: Now to amendment NDP-2.

[*Translation*]

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

The amendment being moved corresponds exactly to the testimony of the Privacy Commissioner of Canada. I think his testimony is essential and must be considered when we study a bill that directly concerns his sector of responsibility. The Privacy Commissioner suggested that the threshold that allows for the sharing of information without consent had to be raised. There has to be more than simple suspicion.

Through this amendment, I suggest that we lift the threshold so that the organization must have reasonable grounds to believe that the information relates to an investigation.

I think that this amendment is greatly needed. I hope the government will accept it, even though we know it does not intend to change the bill and simply wants to ignore the testimony we have heard.

[*English*]

The Chair: Thank you, Madam Borg.

Mr. Lake.

Hon. Mike Lake: Again, in the interest of time and grouping some things together here, I believe there are six NDP amendments in this area of private investigation, fraud prevention. There's one additional Green Party amendment. Maybe I'll ask the officials to comment on that group of amendments so I don't have to go back and forth seven times.

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

This is a recurring theme through about four of these amendments of replacing the standard as proposed in Bill S-4, which is that the investigation or the fraud prevention activities would need to be reasonable for those purposes, with the standard of the organization having to have reasonable grounds to believe that something had happened warranting an investigation, or that fraud had occurred warranting the fraud detection, suppression, or prevention activities.

The second part deals with the last part of the test as proposed in Bill S-4, which says it would be reasonable to expect that disclosure with the knowledge and consent of the individual would compromise those activities.

This group of amendments replaces “reasonable for the purpose” with “reasonable grounds to believe”. The two thresholds are different as I've mentioned in the last response. The “reasonable for the purpose” is an objective standard. Looking at a situation, a court or the Privacy Commissioner would look at the conduct of the organization in the circumstances and look at whether their actions in disclosing the information are reasonable. Did they exercise good judgement? Were they fair? They would look at factors like the sensitivity of the information being disclosed and the seriousness of the conduct that was being investigated, in the case of investigations, or the seriousness of the fraud that was being looked for.

By changing to “reasonable grounds to believe”, it increases the threshold to the point where the organization would have to have compelling and credible evidence that something had occurred that warranted an investigation, or have compelling and credible evidence that fraud had occurred. It's a higher threshold. The reason why Bill S-4 proposes a lower threshold is that the purpose of these investigations in many circumstances, and the fraud protection prevention and suppression activity, is precisely to obtain clear and compelling evidence to meet that threshold of “reasonable grounds to believe”. The organization then can move from “I have a suspicion” or “I have an allegation of wrongdoing” to conduct some sort of internal investigation, determine that there is clear and compelling evidence that wrongdoing had occurred, and then move it to the next level. In the case of a criminal matter, that's referring it to law enforcement or in the case of an agreement among professional associations, such as lawyers or doctors, moving it into disciplinary action against the member of the organization.

● (1130)

The Chair: Is there any other discussion in that regard?

All in favour of amendment NDP-2?

(Amendment negatived [See *Minutes of Proceedings*])

The Chair: Now, Mr. Lake, you had mentioned a grouping. I'm not privy to that information here in regard to this subject, so amendment NDP-3 would be our next one.

Is it germane to the conversation we just had?

[*Translation*]

Ms. Charmaine Borg: Indeed, the same reasoning applies to amendment NDP-2 I presented earlier as well as to NDP-4. The objective is to increase the threshold and ensure that this information will be shared only in situations deemed reasonable.

I repeat that this is in keeping with the recommendations of the Privacy Commissioner. The same is true for amendments NDP-4 and NDP-5. It is extremely important that we take these comments into account since this is a bill that is supposed to protect privacy.

[*English*]

The Chair: Amendment NDP-3, any other discussion in that regard?

Mr. Hyer.

Mr. Bruce Hyer: Thank you, Chair.

Our amendments PV-7 and PV-8 also deal with the same section. I wonder if you might want to have my comments now before further comments or vote.

The Chair: If it pleases everybody here, we'll deal with amendments NDP-3, NDP-4, NDP-5, and yours as well. If that pleases everybody, we'll debate them right now.

Yes, go ahead, Mr. Hyer.

Mr. Bruce Hyer: Mr. Chair, these amendments deal with deleting the lines regarding new warrantless disclosure provisions that go from company to company. As they're drafted in Bill S-4, companies will be able to share the general public's information without our knowledge or consent. Privacy experts are most concerned about this aspect of Bill S-4.

There has been a surge of recent cases of what some people call “copyright trolling”; in other words, companies sending extensive legal letters to customers threatening huge fines for downloading movies that people have never heard of.

As it stands, Bill S-4 would allow involved service providers to offer this information to anyone without the consent of the individual. Therefore, we feel that warrantless, non-notified voluntary disclosures should be removed from the bill.

The Chair: Mr. Clare, do you have something additional in regard to that?

Mr. John Clare: Mr. Chair, I would just point out the difference between these amendments and the NDP's amendments. The NDP amendments propose to change the threshold. These types of disclosures would still be permissible in certain circumstances, but it changes the threshold for when the disclosures would be permitted. This amendment would remove the exception entirely, so it would eliminate any exception to consent for either fraud prevention, detection, or suppression activities, or private investigations.

It's worth pointing out that the amendment in Bill S-4 that provides these exceptions.... They are not new exceptions. They change the way that these disclosures happen. Currently there are provisions in PIPEDA that allow for private investigations. We refer to it as the “investigative bodies framework”. Bill S-4 repeals the investigative bodies framework and replaces it with these exceptions. This amendment takes out the exceptions from Bill S-4, but it doesn't return back to the status quo.

● (1135)

The Chair: Are there any other comments on those amendments?

Just as a reminder to everybody, we're dealing with NDP-3, NDP-4, and NDP-5, and PV-8.

[*Translation*]

Ms. Charmaine Borg: I would like to make one clarification in that regard.

Grouping all of the amendments together was discussed. However, to make things somewhat simpler, we could simply vote on them one at a time.

[*English*]

The Chair: Sure. NDP-3 is the first vote. Shall that amendment stand?

(Amendment negatived [See *Minutes of Proceedings*])

The Chair: PV-8 is the next one that we'll be voting on then.

(Amendment negatived [See *Minutes of Proceedings*])

The Chair: Next would be NDP-4.

(Amendment negatived [See *Minutes of Proceedings*])

The Chair: Next would be NDP-5.

(Amendment negatived [See *Minutes of Proceedings*])

The Chair: Next would be NDP-6.

Madam Borg.

[*Translation*]

Ms. Charmaine Borg: I am not going to spend too much time on this. This is really the same amendment, aside from the fact that we have paragraph *(d.2)* rather than *(d.1)*.

You have already heard what I had to say on this. I think this is an important amendment to ensure the protection of the privacy of Canadians.

Thank you.

[*English*]

The Chair: Are there any other comments?

(Amendment negatived [See *Minutes of Proceedings*])

The Chair: Next is NDP-7.

[*Translation*]

Ms. Charmaine Borg: Through this amendment and with the words "reasonable grounds to believe" we intend to up the threshold. This is in line with previous amendments. I think that this threshold, as proposed by the Privacy Commissioner of Canada, would afford greater respect for Canadians' privacy.

[*English*]

The Chair: All those in favour of NDP-7?

(Amendment negatived [See *Minutes of Proceedings*])

The Chair: Next would be PV-10. It's Mr. Hyer, I believe.

Mr. Bruce Hyer: Thank you, Mr. Chair.

These amendments deal with provisions that would allow the disclosure of personal information to a person's next of kin or their representative. There have been some good arguments for it. However, we are proposing that it be deleted nonetheless, on the advice of the Canadian Bar Association's elder law and privacy and access law sections, for three reasons.

One, it's intended to apply to older adults and as such may be discriminatory. I'm getting closer to that every day.

Two, the list of people and organizations that may receive disclosure without consent is unnecessarily broad and unspecified.

Three, in particular, "next of kin or authorized representative" is problematic, as financial abusers of older adults are most often the next of kin or authorized representatives themselves.

Thank you, Mr. Chair.

The Chair: Thank you, Mr. Hyer.

Mr. Lake, would you like any of the officials to comment?

Hon. Mike Lake: If they want to.

Mr. John Clare: I think Mr. Hyer explained the amendment.

● (1140)

The Chair: All right.

(Amendment negatived [See *Minutes of Proceedings*])

The Chair: Next is PV-12.

Mr. Hyer.

Mr. Bruce Hyer: Thank you.

This amendment is responding to concerns by Michael Geist and what he called the "glaring omission" in PIPEDA, which is that organizations do not need to report on how many warrantless disclosures to the government they've made and they never need to notify the individual whose information has been shared. The number of requests made to telecoms is absolutely staggering—over a million requests, and 750,000 disclosures of personal information—and the majority of those are without court oversight or warrants.

First, the law should require organizations to publicly report on the number of disclosures that they have disclosed, in aggregate, every 90 days. Second, organizations should be required to notify affected individuals of that disclosure within some kind of reasonable time period.

Thank you, Mr. Chair.

The Chair: Mr. Lake.

Hon. Mike Lake: I'll just get the officials to comment on the impact of that.

Mr. Christopher Padfield (Director General, Digital Policy Branch, Department of Industry): This would require all organizations covered by PIPEDA that make any disclosures to law enforcement, any government agency, or any investigative body, for that matter, to record all those exchanges and to notify individuals within 60 days and make a public report every quarter.

That's a significant administrative burden. This would cover every organization covered by the act, so every small business or what have you. Because of the broad nature of the proposed amendment, it would cover any interactions or any exchanges. Take something as simple as a police officer asking someone working in a doughnut shop about a customer who was recently in. The doughnut shop owner would require, under that circumstance, to record that type of information, keep a record of it, try to notify the individual whose information they gave out, and then every quarter report out on those kinds of exchanges.

The Chair: Thank you, Mr. Padfield.

Is there any further debate on PV-12?

(Amendment negatived [See *Minutes of Proceedings*])

The Chair: Those are all the amendments for clause 6.

(Clause 6 agreed to)

The Chair: We now have a proposed new clause 6.1 in amendment NDP-8.

Madam Borg.

[*Translation*]

Ms. Charmaine Borg: Mr. Chair, this amendment is related to NDP-1. It would be illogical to move it since NDP-1 has not been passed. And so, I will withdraw it.

Thank you.

[*English*]

The Chair: Thank you.

(On clause 7)

The Chair: On NDP-9, we have Madam Borg.

[*Translation*]

Ms. Charmaine Borg: The purpose of this amendment is to add the word “reasonable” to the word “necessary”, which was proposed. I think our witness Professor Levin had suggested that. It is a very simple amendment but it would ensure that people will act in a reasonable way when it comes to personal information. Once again, the purpose is to increase the thresholds.

Thank you very much.

[*English*]

The Chair: Thank you, Madam Borg.

Let's go to the officials.

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

To be clear, the language proposed in Bill S-4 is that the disclosure would need to be necessary to establish, manage, or terminate the employment relationship and the amendment would add “and reasonable”.

We've talked about the reasonableness threshold already and what that entails. The fact that subsection 5(3) of the act already provides this overall requirement that any collection, use, and disclosure be reasonable in the circumstances, the use of the term necessary was intended to establish a higher threshold than reasonable.

In other words, the collection, use, or disclosure of that specific personal information is required for the purpose. So it would only be information that is required to establish, manage, or terminate an employment relationship. It wouldn't include any other information in the context of someone's employment.

● (1145)

The Chair: Thank you, Mr. Clare.

Is there any other discussion on NDP-9?

(Amendment negatived)

The Chair: NDP-10, Madam Borg.

[*Translation*]

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

This is in my opinion no doubt the most important amendment I will move today. In fact, this amendment ensures greater transparency. If there have to be exceptions in PIPEDA with regard to the sharing of information without consent, I think it would be essential that there be transparency and that there be a mechanism so that Canadians know how often this happens.

The acting Privacy Commissioner said that 1.2 million requests were submitted to organizations for personal information without consent and without warrants. I know that people are worried because there are gaps and there has been abuse. That is very clear. The acting commissioner said that there was a lack of transparency and that there were no means to oblige the organizations to divulge this information. Even government agencies are not obliged to reveal how often these requests are submitted to them. We must thus ensure that there is no abuse. I think this is primordial.

The amendment specifically asks that a report be published on this. The point is not necessarily to inform individuals, but we can kill two birds with one stone because we will in this way publicly divulge how often this has occurred. I think this is what Canadians are asking for. It is in my opinion very important that this amendment be brought forward today so that the privacy of Canadians will be respected.

[*English*]

The Chair: Mr. Lake.

Hon. Mike Lake: We heard from a lot of witnesses on this, and if anything the witnesses reinforced for me that we found the balance in the legislation that we brought forward. We heard witnesses calling for more and we heard witnesses calling for less. It seems we have a very balanced approach in the legislation. I will of course allow the witnesses to testify to this if they have anything to add.

Mr. Christopher Padfield: The amendment is drafted to cover more than just the disclosures. It covers the collection, use, and disclosure any time anyone collected any personal information of any kind, any time we use any kind of personal information, and any time it's disclosed. All three of those things would be covered by the amendment. It's a very broad capturing for those corporate reports. Companies would be required to report any information of any kind.

Again, this one where it's quite broadly placed would include journalists. They would have to make quarterly reports on when they have collected, used, and disclosed the information.

The Chair: Is there any other debate on NDP-10?

(Amendment negatived)

(Clause 7 agreed to)

(Clause 8 agreed to)

(On clause 9)

The Chair: Clause 9, we have NDP-11.

[*Translation*]

Ms. Charmaine Borg: Mr. Chair, that amendment corresponds to an amendment that had already been defeated. Consequently I will withdraw it.

[*English*]

The Chair: Okay. Does clause 9 carry?

(Clause 9 agreed to)

(On clause 10)

The Chair: The first amendment we'll deal with is Liberal-3.

Hon. Judy Sgro: Mr. Chair, maybe I'll speak to both amendments Liberal-3 and Liberal-4, because they both pertain to the same clause.

Both of these amendments were supported or proposed or contributed to by several witnesses, including those from the Insurance Bureau of Canada. They deal with the reporting threshold and the remedies for breaches.

Amendment Liberal-3 to clause 10 would require the reporting of any breach of security so long as said breach presented a real and significant threat of harm to an individual. The proposed amendment also clarifies the remedy associated with the breach.

If I can speak to amendment Liberal-4 on the same clause, this amendment was supported and proposed again by several witnesses, including those in the Insurance Bureau, and it requires that, unless otherwise prohibited by law, an organization shall, in accordance with any prescribed requirement, keep and maintain a record of every material breach of security safeguards involving personal information under its control. This amendment clarifies the previously broad nature of the provision and acknowledges that this legislation must exist within the context of a more complex system of law.

I was actually going to ask the department to comment on those two proposed amendments and what they attempt to do, which is to provide further clarification.

Would you like to elaborate on that?

● (1150)

Mr. John Clare: The amendment has two parts. Many witnesses came before this committee and talked about the threshold for when organizations would be required to report a privacy breach to the Privacy Commissioner and the thresholds for when they would be required to notify individuals. That's the substance of the first amendment.

The proposed amendment would create two thresholds. For a report to the Privacy Commissioner, the breach would need to be a material breach. The criterion for a material breach is essentially that there's an aspect of risk, but I would argue it's designed to be a less objective test. You do look at the sensitivity of the information, but primarily you look at how many individuals were affected. Then the organizations do an internal review, and they ask whether this represents a systemic problem and whether it is evidence that they have a bigger problem here that they should tell the Privacy Commissioner about.

The other threshold is, as proposed in Bill S-4, the notification to individuals. This is unchanged. It would be a breach that is determined to pose a real risk of significant harm. This is a risk-based threshold. We look at the circumstances, the sensitivity and the probability that the information will be misused and the potential harm that it could cause, and those are the breaches we would tell individuals about.

It establishes these two thresholds, so what the Privacy Commissioner would be told about wouldn't necessarily be the same data breaches that individuals would be notified about.

From my own perspective what I found interesting about the testimony that the committee heard is that, on the one hand, business organizations like this because they don't want to have to tell the Privacy Commissioner about the one-off breach, the one that was really serious but only affected four or five people. They wonder why they need to tip off the Privacy Commissioner that this has happened. They'd rather only tell the Privacy Commissioner about the big problems, and deal with these with their clients directly.

Privacy advocates, on the other hand, didn't see these two thresholds as necessarily different. They saw them as nested in some way, so that the material breach was actually a lower threshold and that the Privacy Commissioner would hear about all of those breaches that affect one-offs—two or three people. But then for the ones that go to the individual, it's a higher threshold of that higher risk. They saw it that way.

From a policy perspective and as administrators of the law, the fact that you saw those two different views suggests that the provisions are not necessarily as effective and clear as they could be, if you have different stakeholder groups interpreting them in very different ways.

The committee may be aware that those two thresholds, the material threshold and the real risk threshold, were in previous versions of government bills to amend PIPEDA. But when Bill S-4 was drafted, this issue was examined and it was determined that because of those competing views, it was more simple, more effective for there to be a single threshold. An organization would look at a data breach and they'd say, “Is there a risk of harm in this circumstance? If there is, I have to tell the Privacy Commissioner and I have to inform the individual.”

That way the Privacy Commissioner knows about every single data breach that goes out to individuals. But to create accountability and to make sure that organizations are conducting these risk assessments in good faith, Bill S-4 creates a new requirement that wasn't in previous bills, and that's to maintain the records.

The process is very straightforward. I have a data breach. I determine if there is a risk. If there is, the notification goes out. If the determination is that there isn't a risk, that this may be evidence of a systemic problem or something like that, I have to maintain a record. The policy rationale behind that is that as soon as you require an organization to record this information and maintain it, they're going to pay more attention to it and this is how they're going to determine whether or not they have a systemic problem.

Bill S-4 gives the Privacy Commissioner the power to demand those records at any point. There's no threshold. The commissioner doesn't have to have any suspicion that something's going on. He can ask to see a company's records.

This gets to the second part of the amendment, which deals with that record-keeping requirement.

● (1155)

The committee heard witnesses saying that they were concerned about this requirement. What information were they going to have to maintain in the record? How long were they going to have to keep it for? They were nervous about the burden that it would create. The only thing I would point out to the committee is that all of those specific requirements will be set out in regulation, and there will be an opportunity to consult broadly with it.

The intention of the record-keeping requirement is to maintain only that information that's necessary to meet those two objectives I talked about: making sure the company pays attention to it, and providing a way for the commissioner to hold the company accountable for that risk assessment.

To the extent that the requirement to document a data breach may create a conflict in law that may be contrary to some other law, we're not aware of any federal statute that would prohibit a company from documenting that they have suffered a data breach. As for the specific requirements, if there was concern that there may be a conflict in law if the regulations, say, you have to keep it for five years and there is some other requirement that says you have to destroy these things after two years, all of that would be addressed during the regulatory process and it wouldn't be necessary to have that chapeau in the act saying unless prohibited by law.

The Chair: Mr. Hanson.

Mr. Lawrence Hanson (Assistant Deputy Minister, Science and Innovation, Department of Industry): I just would add one additional contextual point that I think may be helpful in terms of the discussion of data breach writ large. When we think of private sector privacy law, we often tend to think of the capacities of large telecommunication companies or financial institutions, but I think it's valuable for the committee to bear in mind with this legislation that small and medium-sized enterprises are also required to abide by PIPEDA.

An additional reason for this, beyond those that my colleague has explained, is that by having a single threshold, you do not force individual small and medium-sized firms, which may not have the same capacity or access to legal advice, etc., to have to sort of arbitrate or adjudicate among different standards, but rather just have a single, clear standard they are able to follow. I think that's another explanation for the single threshold.

The Chair: Thank you, Mr. Hanson.

Is there any other discussion on Liberal-3 and Liberal-4?

We'll vote on them separately. First, we will have Liberal-3.

(Amendment negatived [See *Minutes of Proceedings*])

The Chair: Now we'll vote on Liberal-4.

(Amendment negatived [See *Minutes of Proceedings*])

The Chair: We're still on clause 10. Next will be NDP-12.

[*Translation*]

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

In testimony on Bill S-4 we heard a lot of different opinions on the implementation of a notice mechanism for data breaches. This is a contentious point. In fact I examined this at length when drafting my bill. I am referring here to Bill C-475 which was unfortunately defeated because of the Conservative Party.

Through this amendment, I want to propose a more objective threshold. Indeed, I would like the Privacy Commissioner of Canada to be responsible for assessing the prejudice the person whose data has been lost, breached, and so on could suffer.

This legislation does not only apply to large businesses, but also to small ones. However, small enterprises do not necessarily have the necessary means to determine if the data breach is serious. These businesses could turn to the Privacy Commissioner of Canada. He knows these issues and is in a position to determine whether the data breach justifies notifying the person.

Moreover, this amendment would allow the Privacy Commissioner of Canada to order organizations to inform the persons concerned. This would also force organizations to notify people and would give the commissioner a little more power. Indeed, he could ensure that the privacy of individuals dealing with the organizations is respected.

I think this threshold is more objective, that it would afford better privacy protection, and that it would reduce the burden on small businesses.

Thank you.

● (1200)

[*English*]

Hon. Mike Lake: I'll just ask the officials if they have anything to add from the last conversation we had.

Mr. John Clare: Let me just point out to the committee how what is proposed is different from having the organization do an assessment of two thresholds in making that determination. As Madam Borg pointed out, the NDP amendment does create a two-step process, so an organization would first determine whether or not a breach posed a possible risk of harm and that would go to the Privacy Commissioner. Then the Privacy Commissioner would look at the data breach and determine whether or not notification to individuals was warranted.

The standard applied by the Privacy Commissioner would likely result in an appreciable risk of harm. The organization is accountable for telling the Privacy Commissioner, which creates an accountability on the part of the Privacy Commissioner to do a risk assessment and determine whether or not individuals will be notified. Bill S-4 places the accountability for both of those things on the organization itself.

Madam Borg's second point was that the amendment gives the Privacy Commissioner the power to order a company to notify individuals, whereas under PIPEDA currently and under Bill S-4, the Privacy Commissioner doesn't have the ability to make those orders.

The Chair: Thank you.

Is there any other discussion on amendment NDP-12?

(Amendment negatived [See *Minutes of Proceedings*])

Next will be amendment PV-14.

Mr. Hyer.

Mr. Bruce Hyer: This amendment reverts back to the proposed language for notifying the Privacy Commissioner about security breaches, which is found in the previous PIPEDA reform bills C-12 and C-29, but it is stronger and clearer. Why? It creates a mandatory security breach disclosure requirement at the federal level, and that is long overdue. Geist at the Senate said that Bill S-4 establishes the same standard of "a real risk of significant harm" for both notifying the commissioner and the individuals, but also said this is very puzzling. It means that there is no notification for systemic security problems within an organization. This is very likely to result in significant under-reporting of breaches. Our amendment creates incentives for organizations to better protect that information and allows Canadians to take action to avoid risks including identity theft.

The Chair: Thank you, Mr. Hyer.

We'll turn now to the officials.

Mr. John Clare: I would just point out to the committee that there are three Green Party amendments that all relate to the data breach provisions, and as Mr. Hyer pointed out, this creates that separate threshold for notification of the Privacy Commissioner as the Liberal amendment did.

The Chair: All those in favour of amendment PV-14?

(Amendment negatived [See *Minutes of Proceedings*])

Would you like to speak to amendment PV-16, Mr. Hyer?

Mr. Bruce Hyer: These amendments lower the threshold at which an organization has to notify an individual about a breach. Instead of there being a judgment that there's a high risk of harm, an individual has to be notified if their information has ended up in the wrong hands.

For example, the California breach notification law requires disclosure of any breach of unencrypted personal information that is reasonably believed to have been acquired by any unauthorized person.

● (1205)

The Chair: Mr. Lake.

Hon. Mike Lake: I'll go back to the officials again.

Mr. John Clare: Mr. Chair, the only thing I would point out to the committee is that, as Mr. Hyer points out, this eliminates a risk-based threshold and essentially replaces it with a requirement to notify individuals if the organization believes that some unauthorized person has accessed the information.

I would make two points. One is that the Privacy Commissioner testified before this committee and has long advocated for a risk-based approach, recognizing that we don't want to tell individuals about data breaches that don't actually pose a risk of harm. You want them to be told of those that they need to pay attention to, because part of the objective of notifying people is getting them to take action to mitigate or reduce the risk of harm, such as changing their PIN, calling their bank, and monitoring their credit card statements. If you create a system whereby individuals are constantly being notified of breaches where there isn't necessarily a risk of harm, you run the risk that they'll stop paying attention to them and they won't take the action that you want them to take.

The second point I would make is with respect to the California data breach law. The personal information covered by that law is much narrower than under PIPEDA. Under PIPEDA, the definition of "personal information" includes any "information about an identifiable individual", so a lot of non-sensitive information is included, whereas the California law has a very specific subset of personal information, which is risky. It is highly sensitive information. Read together, it makes more sense that the California law applies to all data breaches and doesn't take this risk approach, because it already narrows what personal information it covers.

The Chair: Thank you, Mr. Clare.

All those in favour of amendment PV-16?

(Amendment PV-16 negatived [See *Minutes of Proceedings*])

The Chair: Those are all the proposed amendments for clause 10. Shall clause 10 carry?

Hon. Mike Lake: Wasn't there one more? He still has one more.

The Chair: I'm sorry, Mr. Hyer. Please go ahead.

Mr. Bruce Hyer: No problem, Mr. Chair.

These amendments deal with the lines that greatly expand the regime of warrantless disclosure to law enforcement and government agencies. Canadian telecommunications providers that collect massive amounts of data about their subscribers are asked to disclose basic subscriber information to Canadian law enforcement agents every 27 seconds. In 2011 alone, that added up to over a million disclosures.

Warrantless disclosure, in proposed subsection 10.2(3) and Bill C-13, plus the information-sharing provisions in Bill C-51, create an extremely worrisome system of surveillance, opening the door for a more Big Brother sort of government.

The Chair: Thank you, Mr. Hyer.

Mr. Clare.

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

I would point out to the committee that this exception to the requirement for consent is very narrow. It's very specific to a data breach scenario. Experience has shown that when a data breach occurs, the ability of an organization to share the fact that information has been compromised with other third parties allows them to mitigate or reduce the risk of harm.

The perfect example is a retailer that has the credit card numbers of their customers compromised and exposed in a breach. The retailer, by notifying the credit card company, could reduce the risk of harm by saying that they have had 50,000 credit card numbers compromised. The credit card company can put a flag on those accounts, monitor them for unusual activity, and actually help the retailer identify the contact information for those individuals so they can go out and directly notify them that a data breach has occurred.

What this provision does is provide an exception only in that circumstance. When you're disclosing personal information to a third party in the context of a data breach so they can help reduce or mitigate the risk of harm, you don't need to get consent to do that. In my example, you don't need to go to the customer and ask if it's okay to tell the credit card company that the customer's credit card has been stolen.

The Chair: Is there any other conversation? Those in favour of amendment PV-18...?

(Amendment PV-18 negatived [See *Minutes of Proceedings*])

The Chair: Ladies and gentlemen, I'm pretty certain now that these are all the proposed amendments for clause 10.

(Clause 10 agreed to)

(Clauses 11 and 12 agreed to)

The Chair: We're now on amendment NDP-13.

● (1210)

Ms. Charmaine Borg: I just want to specify that this is a corresponding amendment to a future amendment. It's a little bit tricky because we haven't voted on the other amendment yet. The overall intent here is to give the Privacy Commissioner more powers, specifically order-making power, so that we can force organizations that aren't complying with PIPEDA to have an incentive to comply by the commissioner's investigation resulting in something more than a simple recommendation—an order that would be respected.

Now, I understand there are some good actors and we definitely want to encourage organizations to not have to get to the point where there's an order that's made or that there is some good will. There's a lot of good will out there. I think the series of amendments I want to put in place allow organizations, following the commissioner's order, to have a certain delay to be able to comply with that order without there being any repercussions. After that, obviously there is some wiggle room for some exceptions and some time extensions to be applied, but if the organization has not complied with that order within a certain amount of time, the commissioner would have the ability to bring that matter to court, which could then impose fines. We've heard this from multiple privacy advocates. This is very important because what we're seeing right now, especially in this age of big data where we have international organizations coming into Canada, is Canadians using these services but then completely disregarding any recommendations coming from the Privacy Commissioner's office. It's extremely problematic.

I see I'm supposed to speak to this amendment, but I guess I'll just speak to NDP-14 too because they are related. I think we need more than just compliance agreements. I think compliance agreements are a good start, but they don't go far enough. They don't go far enough to ensure that the Privacy Commissioner has the powers that he needs to be able to make sure that PIPEDA is being enforced and for organizations to have real incentives to respect the privacy of Canadians, which unfortunately is not happening right now. We've heard witnesses say the compliance agreement is a good start. I think everyone will say that, but we need to go further to ensure in this age of big data that privacy is protected.

I'm just going to perhaps specify that I'll speak to NDP-14, and I guess NDP-15 at the same time, then. I'm speaking to NDP-13, NDP-14, and NDP-15 altogether since they're very much related.

Thank you.

Hon. Mike Lake: I will, not surprisingly, ask the officials to comment on all three of those amendments—NDP-13, NDP-14, and NDP-15.

Mr. Christopher Padfield: It may also be useful to consider NDP-16 and NDP-18. I think they're all part of the same order-making framework.

Just on the context of order-making powers, it was an issue that was discussed during the first parliamentary review. During the review they found that the current ombudsman model wherein the commissioner works cooperatively with organizations has been very effective in addressing issues.

I think that's evident in the recent Bell case. People are familiar with the relevant advertising program that Bell has been operating where they were collecting personal information about their customers from various sources, so their television watching habits, their telephone use habits, tracking their Internet browsing habits, and anonymizing it all by creating these profiles that they were attaching to other demographic information. The commissioner, after 170 complaints he received in 2013, undertook a broad-based review. I know, having had discussions with officials from Bell, there's a lot of back and forth with Bell and the commissioner's office, and the commissioner came out with these findings and asked that Bell fundamentally change the model, which had been an opt-out approach, where individuals would have to actively decide not to and could not decide to opt in to the proposal.

They also asked the commissioner to give another series of recommendations, all of which Bell complied with. If one looks over the history of PIPEDA and the number of times the commissioner has actually had to take anyone to court, there have been 17 occurrences over the full course of PIPEDA. Of those, 16 were settled before court, and on the 17th, the commissioner actually lost the case in court. There has not been a whole host of activity going towards court under the current model and I think it's shown, with Bell being a good example, how effective that's been.

● (1215)

The Chair: Is there any other discussion?

Madame Borg.

Ms. Charmaine Borg: Thank you.

I'd like to add, following Mr. Padfield's comments, that there has been testimony from previous privacy commissioners that the current court process is extremely complicated and often very troublesome for the Privacy Commissioner's office to go forward.

You can comment on that if not.... Perhaps we have different opinions about that as well, which is fine.

Mr. Christopher Padfield: To add, I think that's part of the rationale in Bill S-4 and the additional powers that were given to the commissioner with that longer period of time to go to court. Under PIPEDA previously, it would have been 45 days, but Bill S-4 extends that to a year. It gives the commissioner more of a timeframe to go in.

It also expanded the commissioner's name-and-shame powers, if you like. The commissioner can more publicly report on a broad range of activities that companies are undertaking, which I think was one of the issues in the Bell case. The commissioner made his findings public, which he's not required to do, but he thought it was in the public interest to make them public.

I think Bill S-4 provides additional authorities and powers that still fall within that ombudsman model that has been so effective, and doesn't move the commissioner into a regulator role and more of a conflictual role with the private sector.

Ms. Charmaine Borg: I have perhaps one more comment.

I'm not sure if it would be appropriate to consider NDP-16 at this time, since it would be after clause 16 that we should consider it.

I don't know how you want to—

The Chair: We can vote on those now.

Ms. Charmaine Borg: Okay.

I would like to speak directly to NDP-16, if that's okay.

Hon. Mike Lake: I think the witnesses referred to all them up to 18, so do you want to do NDP-16 and NDP-18 at the same time?

Ms. Charmaine Borg: NDP-17 and NDP-18 don't—

Hon. Mike Lake: NDP-17 is in a different area but NDP-18 kind of fits in the same category, does it not?

Mr. Christopher Padfield: Yes.

Ms. Charmaine Borg: That's fine. We can link in with that as well.

I don't know. It's because they're different clauses.... That's the only reason I would have separated them.

I would like to speak to NDP-16 because I think it's important as part of the package of amendments that I'm trying to put forward in order to give the Privacy Commissioner order-making powers. We all know that the Privacy Commissioner can conduct an audit when there is some indication that there may be some violations of PIPEDA. This amendment seeks to include any orders that would follow an audit and recommendations to be made public. It is in a certain sense a corresponding amendment, but I think it is an important one because it would make those orders public. Again, name-and-shame power is important, so that kind of ties into there.

Thank you.

The Chair: And on NDP-18, Madam Borg?

Ms. Charmaine Borg: It's a very technical amendment. I don't see the necessity to speak directly to it.

The Chair: Okay.

We'll now then consider NDP-13, NDP-14, NDP-15, and NDP-16, but we'll vote on them separately.

All those in favour of NDP-13?

(Amendment negatived [See *Minutes of Proceedings*])

(Clauses 13 and 14 agreed to)

The Chair: Now we have amendment NDP-14.

(Amendment negatived [See *Minutes of Proceedings*])

(On clause 15)

The Chair: We have NDP-15, which has already been addressed.

(Amendment negatived [See *Minutes of Proceedings*])

The Chair: Now we'll go on to PV-20.

● (1220)

Mr. Bruce Hyer: Thank you.

Mr. Chair, this is essentially a reiteration of Madam Borg's Bill C-475, which we think is a great model on this topic and we would like to acknowledge her hard and competent work on this file.

The creation of compliance agreements is a step in the right direction, but order-making powers need some form of direct regulatory action such as administrative and monetary penalties. Without such an incentive—you might even call it a threat—it is difficult to see why an organization would enter into such an agreement. Reforms are needed, with real penalties to ensure compliance.

Thank you, Mr. Chair.

(Amendment negatived [See *Minutes of Proceedings*])

(Clause 15 agreed to on division)

(Clause 16 agreed to on division)

The Chair: NDP-16 has been addressed by Madam Borg. Is it okay to go ahead and vote on it, Madam Borg?

Ms. Charmaine Borg: Yes.

(Amendment negatived [See *Minutes of Proceedings*])

(Clauses 17 to 20 inclusive agreed to on division)

(On clause 21)

The Chair: We're on clause 21, and we have NDP-17.

Madam Borg.

Ms. Charmaine Borg: I think at this point, because these amendments, NDP-17 and NDP-18 are corresponding amendments to other amendments of mine that were already defeated, they're strictly irrelevant. I will withdraw them.

The Chair: Thank you, Madam Borg.

(Clause 21 agreed to on division)

(Clauses 22 to 27 inclusive agreed to on division)

The Chair: Shall the short title carry?

Some hon. members: Agreed.

An. hon member: On division.

The Chair: Shall the title carry?

Some hon. members: Agreed.

An. hon member: On division.

The Chair: Shall the bill carry?

Some hon. members: Agreed.

The Chair: Shall the chair report the bill to the House?

Some hon. members: Agreed.

The Chair: Colleagues, thank you very much, and to the officials, thank you very much for your expertise.

As there is no other business, we'll be adjourned.