House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 032 • 1st SESSION • 39th PARLIAMENT

EVIDENCE

Tuesday, February 20, 2007

Chair

Mr. Tom Wappel

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, February 20, 2007

● (0915)

[*English*]

The Chair (Mr. Tom Wappel (Scarborough Southwest, Lib.)): Good morning, everyone.

We have today only one set of witnesses, the Royal Canadian Mounted Police, in the persons of Bruce Rogerson, assistant commissioner; Art Crockett, officer in charge of strategic services branch, technical operations; and Earla-Kim McColl, officer in charge, national child exploitation coordination centre.

Welcome to you all. You will have approximately ten minutes for opening remarks, and then we'll go right into questions. Thank you for requesting to appear. We're looking forward to your evidence.

A/Commr Bruce Rogerson (Assistant Commissioner, Royal Canadian Mounted Police): Good morning. Thank you.

It's a pleasure to be here this morning to at least clarify what we feel is a correction that needs to be made in the PIPEDA legislation, which will allow the RCMP to collect informal information in a more congenial fashion and allow us to do our day-to-day job.

Obviously the RCMP is one of your national police forces, but it's also the uniform police service across Canada. We service eight provinces, three territories, we're in over 200 municipalities, and we're throughout Canada in over 700 locations.

However, having said that, through the feedback we're getting through our membership, the RCMP has increasingly encountered challenges with respect to the changes invoked under PIPEDA five years ago, especially when it comes to collecting information from the private sector and private organizations. which, prior to the revisions of five years ago—was freely permitted to receive, and very seldom met with any rebuttal from our colleagues.

I can tell you that in my interactions with the communities and civic duty throughout Canada over the last 33 years, I have found that we have an excellent relationship in general in a majority of cases with the communities we serve, and also with the organizations and public institutions that we request information from. That has been proven in many surveys, where our client satisfaction, which includes the business community, rates well above or close to 92% on an annual basis. So there is an element of trust between us and our service delivery.

However, there is confusion now amongst the organizations when we deal with them and ask them for information that in reality is just information at the beginning of any review or any instance whereby we receive information. It's like gathering a 1,000-piece puzzle. We really don't know what we have when we seek such information. In gathering those pieces of the puzzle they add up to a point where we feel it's either criminal or non-criminal, and then we move in to the criminal side, where search warrants and that are required. However, under PIPEDA in recent years we have found that the changes to sections 7 and 9 have made it a little more confusing for the partners we're dealing with on a day-to-day basis to ensure we prevent crime and provide safe homes and safe communities throughout Canada.

I would say that it's well publicized because of the wording in section 7 that deals with lawful authority. Many people have defined that to mean court-ordered, or court documents, and therefore they have refused to provide simple customer name and address and simple information that was obviously provided before. So there's real confusion around that terminology under section 7. We can talk about the well-publicized case in St. Thomas, Ontario, whereby a suspect was identified and an Internet service provider did provide the information without a warrant, which was under his discretion and his definition of lawful access. Therefore the police were able to glean enough information in the early stages to get a search warrant and therefore apprehend the individual, who was assaulting a very young lady.

In a recent case in British Columbia, a person with Alzheimer's disease walked off, he had a medical alert bracelet, and the people we called to glean information on that individual told us that they weren't allowed to give us the information without a court authorization. So even in a medical alert, where we deal with people who may have epilepsy and stuff like that, you need to know whom you're dealing with, even at the very front line. So it deals with members at the front line, serious crimes, child exploitation, and also the protection of other individuals.

With respect to the warrant aspects, we have had some case law whereby the information that we seek under PIPEDA really is not described as information that warrants a search warrant. It has been ruled on in three different cases in the early nineties and just before that, whereby the customer name and address are not really considered a violation of one's rights under the Charter of Rights and Freedoms.

● (0920)

What we're trying to do under section 7 is readjust the yardsticks, back to where they were prior to the present legislation, to get back to where the interpretation under section 7 is really about giving organizations the permission to provide us that information in the performance of our duties and at the same time transfer the risk back to us.

Obviously, a lot of organizations feel that if they provide that simple information they're putting themselves at civil risk. What we're trying to do is say, no, for them as corporate citizens—it's almost like the good Samaritan situation under first aid—it's permissible to give us that information, and we take on the risk if we misuse it and abuse it.

So one of the things we're looking at is clarity under section 7. We'd like "lawful authority" to be redefined to say that it is permissible to provide information to those acting in accordance with the performance of their duties without a court order or without any authorization from the judiciary.

As I move on to section 9, I guess the same thing could be said with respect to some of the changes whereby a person can call to find out whether information has been released. In that regard, sometimes early on in our investigations we're not sure what we're looking at.

If we're in a major city and somebody is buying two tonnes of fertilizer and we would like to know their name, I could say, for example, that if we accessed their name, we would prefer that the supplier not call the individuals to let them know we had accessed their name, because we're analyzing the information to determine where we're going with it. Also we would like the privilege of being able to instruct the organizations not to release the information until they hear from us any further on that particular issue.

Sections 7 and 9 provide basically our reason for being here today; it's to clarify and to allow us to perform our duties on a daily basis in a more informal and collaborative manner with the citizens we serve, and with the citizens by reflection—the organizations—that we seek personal information from.

I won't go through all of my speaking notes. They're in front of you today, but that is the key message I'd like to give.

I would say that there are issues around regulations about how we act. We have a lot. We have the RCMP Act, as you know; there's a code of conduct in there. If members access information for personal use, and not in line with the duties they perform on a daily basis, they can be reprimanded, they can be fined, they can be dismissed, depending on the degree to which they use the information.

That goes right down to accessing CPIC to find out whether your neighbour has an outstanding warrant or a criminal charge against them, or whether they have a criminal record. If we find out, members are reprimanded, and as to the degree of severity, we deal with our members internally.

So we have the internal one, we have the Criminal Code for abuse of process and breach of trust, we have the PIPEDA legislation, we have our *Sources of Federal Government Information*, which also directs us not to misuse information. We have our secret offences act; as an officer today and long after we retire, up until our death, we're not allowed to disclose information.

You also have the Public Complaints Commission. If there's an issue wherein we've abused our authorities, the public has the access to go to the Public Complaints Commission, which has full access to our files and records, to see whether we were derelict or overly aggressive or abused someone's rights under the Charter of Rights and Freedoms.

Along with my colleagues Superintendent Earla-Kim McColl and Superintendent Art Crockett, I hope today to address specific questions and give examples to heighten your awareness as to the impediments the present wording has imposed upon us, from those of a serious nature right down to those of a local nature with respect to the day-to-day operations of our law enforcement service.

● (0925)

The Chair: Thank you, Assistant Commissioner.

We heard about this issue, specifically the definition or lack of definition of law enforcement, last week. Committee members were interested in specific examples, and we very much appreciate the fact that you were able to give specific examples of what you perceive to be the problem with the lack of definition of "lawful authority" and some of the interpretation of section 9.

The usual situation will apply. We have a first round of seven minutes per member—that includes the questions and answers. Then we have a second and third round of five minutes each.

We'll begin with Mr. Dhaliwal, for seven minutes.

Mr. Sukh Dhaliwal (Newton—North Delta, Lib.): Thank you, Mr. Chair, and thank you, officers, for giving us your presentation.

I went through this presentation and deliberations you made to us, and looked at the two perspectives you are coming from. I certainly agree with you on those. With regard to ISP providers, if you don't get that information, child abuse can be on there. On the other hand, you say if the general public had access to the information on the investigation you are undertaking, there might be circumstances where it might also benefit the public.

Can you draw a line where they have access to the information you are investigating? Air India, for example, is a perfect case scenario. PIPEDA wasn't even in effect at the time.

The grave perception in the community right now is that the RCMP and CSIS...you know, you did not have the collaboration, or there wasn't enough public access to those investigations, and we would have avoided that big incident at that time. And there might be some other cases where the public might have some access to the investigation you are undertaking.

What is your opinion on those circumstances?

A/Commr Bruce Rogerson: If you are talking about open source information on the ISPs, which is available to the public, yes, you are right. It's where our tech crime people use information and analyze it to determine whether there is any criminality, whether there's a financial institution at risk, to alert them that we have seen this open source information on the Internet.

With respect to child exploitation—I'm sure the superintendent will talk about that in a minute—even as speak here at this committee, it's going on right now.

With respect to the exchange of information between CSIS and the RCMP, CSIS gathers intelligence in a less informal way, and not with respect to criminal issues within Canada. They look at national security issues when they gather information. When it becomes criminal, they will share that information, because now it moves into our mandate. Vice-versa, if we have intelligence that should be shared with them with respect to national security issues, then we have mechanisms by which we share with CSIS.

I'm in technical operations. A lot of the technical tools we develop are shared with CSIS with respect to how we use technology and surveillance and whatever. We have an excellent relationship with CSIS with respect to the MOUs in place for exchanging technical tools that allow them to do their jobs as well. It depends on the level, because each of us has a different mandate. We are law enforcement, and they are intelligence gathering for national security, whereby they brief the PCO and allow them to know of an impeding threat or a possible threat to Canadians as a whole. The RCMP, on the other hand, are guided by the various statutes and regulations along with the Criminal Code, as far as law enforcement is concerned.

I would say the collaboration in the recent arrest in Toronto would heighten the fact of how integration.... We worked well with not only CSIS but also multiple police agencies.

I hope I answered your question.

● (0930)

Mr. Sukh Dhaliwal: The particular example you took with CSIS, how would the investigation—? You were saying the section 9—you know, when you disclose the information, or the client's information is disclosed, when you are investigating on something. I'm talking about generally, the investigations that the RCMP are doing. Do you think it's in the best interest of the public to know those under access to information?

A/Commr Bruce Rogerson: The reality is that we are the public. The public entrusts us to gather that information on their behalf in the execution of our duties.

I don't believe all information should be accessed, no, by the public in general. Obviously some tightening up needs to be done with respect to privacy, now that we are getting into identity thefts and other areas. What the general public has access to as opposed to what we have access to—those are two different scenarios.

We are accessing the information under lawful authority, based on the Criminal Code and the other acts that guide us and our oath of office as well. The general public is not held up to the same level of scrutiny or same level of accountability as we are on a day-to-day basis.

Mr. Sukh Dhaliwal: Do you see any breaches in duty when you have access to public information? There are some cases when the police might have breached their duty, from the Canadian public's perspective.

A/Commr Bruce Rogerson: I've not really seen breaches. We're very cognizant of the fact that the justice system determines what evidence comes in and what evidence gets thrown out. If they feel that information we gleaned required a judicial order, they will dismiss that evidence. We have a watchdog called the justice system when we glean information or gather that open source information and informal information.

That's why I say that there comes a point in time when, all of a sudden, we've gleaned enough information to establish that there is a criminal act or a possible criminal act. Then we use that information, in reality, to write the search warrant. In other words, we can't go with the cart before the horse. What we do is we gather that information. The information we gather informally allows us to develop what we need in order to get a search warrant.

In a lot of cases, as you know, we don't know if a search warrant or a criminal act is in place. It could be just a simple issue. It could be a missing child. It could be a missing person. Or it could be under the national sex offender registry—we want to know if a certain person stayed at a hotel that day, because they shouldn't be travelling outside their jurisdiction without notifying the local authorities, because they need permission to do so. So we need to know if a pedophile stayed in a local hotel that evening, and if we don't have access to that information, or if the hotel interprets PIPEDA, under its present standing, to say that, no, we need a search warrant, well, we have no grounds for a search warrant, because we're fishing. We don't even know if the person stayed there.

I know, being before a justice of the peace.... I mean, search warrants now run eight or nine pages. A part VI could run you 1,000 pages if you want to get a wiretap.

Right now, all we're looking for is that the industry be allowed—and have a little more clarity in the wording—to say that it is permissible to provide us that information. Superintendent Crockett was one of the builders of the national sex offender registry legislation, and of course, Superintendent McColl is doing the missing children and the child exploitation. But I have proceeds-of-crime people here with me as well.

● (0935)

The Chair: Thank you.

Monsieur Vincent, sept minutes.

[*Translation*]

Mr. Robert Vincent (Shefford, BQ): Thank you, Mr. Chair.

Thank you for being here this morning. I found the way you presented this to us interesting. It was clear and precise, and you cited women and children as examples. But you'll have to go further because what you're requesting in sections 9 and 7 goes much further than that.

You've presented the good side to make us aware of the issue. Ultimately, in the case of pedophiles, we could give you freedom to investigate in order to obtain information. However, that would open the door to all other investigations. However, public trust in your service has crumbled in recent years. Having read the O'Connor report, I can tell you that you're loosening the reins a little too much. Information is being shared left and right. In that sense, your service has some deficiencies.

I know your book contains disciplinary measures. However, are you going to tighten up your watch over the information given to you so that it remains in your service and can't be used or shared and that what has happened does not reoccur?

This is not the first time this kind of thing has happened. I read the document that is distributed to all members every year on complaints concerning the RCMP. It's quite thick. So there's a lot of work to do. I'd like to know what you intend to do to better protect the personal information that you're going to gather from any agency and anyone.

A/Commr Bruce Rogerson: We started by giving a course to certain investigators who have the power to obtain this information in order to determine whether a crime or terrorist act has been committed. I recently wrote a memo to officers in Ottawa to ensure that each one thoroughly knew his citizenship protection role. That memo was also distributed to all officers and managers across Canada. This week, senior managers and the commissioners intend to establish the steps for controlling information, particularly information concerning terrorism, organized crime and other similar types of organizations.

In Montreal, street gangs are our primary concern. We work with the Montreal police every day. Our goal is to reduce and destroy street gangs in order to protect not only young people, but also older people and all other citizens. Even though we have regulations governing the use of personal information, some individuals use that information as they wish. We usually conduct an investigation the moment we realize that someone has used personal information.

Mr. Robert Vincent: By giving that power to police officers, don't you think they'll freely use all the information they can obtain? Any police officer could then request personal information from anyone on this or that person, and they'd be required to give it to them. When they request information, do your police officers talk to the person about the crime that another person might have committed?

A police officer can't communicate information on the investigation he is conducting to the person from whom he requests information. Is that correct? If you don't talk about the investigation, do you simply tell the person that you're requesting information because a crime has been committed or something else? You tell that person that you're a police officer and you ask him to provide you with information on another person. Is that your way of proceeding? Do you provide any details on the investigation, or do you limit yourself to the specific information you want to obtain?

● (0940)

A/Commr Bruce Rogerson: At first, it's really difficult to determine whether there has been a crime.

Mr. Robert Vincent: You have a specific reason for requesting personal information from a third party. I suppose you don't simply want to know that person's address and social insurance number.

[*English*]

Supt Art Crockett (Officer in Charge, Strategic Services Branch,Technical Operations, Royal Canadian Mounted Police): Much of the information we seek is information that is very basic, and it's on general inquiries. It's not that we seek the core personal information of individuals. The information we are discussing in relation to PIPEDA is more basic information.

By way of an example, if there was a serious crime that happened in a hotel and when we arrived there was a dead body in the hotel, if it was on a street, we would go to the neighbours and see if they'd heard anything. So in that inquiry we would go to the hotel management and ask, can you tell me who was in each room, and did you hear anything? That information would not be considered by us, or generally by Canadians at large, as being protected under our charter, protected core information.

So it is that type of information we are discussing, as opposed to the information that is personal that we might need for an investigation. For information that is more personal, we utilize other mechanisms and tools to do that.

It has been my experience across Canada that the public and private sectors want to help; they want to get involved. All they are looking for is a mechanism that will allow them to provide us that very basic information. I can say who was in that room or I can not. What we're seeking is just some clarity so that they know they can be protected. We will be accountable for what we do with that information. It's just the information to protect those people.

Does that help?

The Chair: Merci, Monsieur Vincent.

Mr. Martin.

Mr. Pat Martin (Winnipeg Centre, NDP): Thank you, Mr. Chair.

Thank you, witnesses.

Building on what my colleague from the Bloc was asking, my understanding was that PIPEDA under section 7 already allowed or permitted organizations to use personal information without knowledge or consent.

The change made when the Public Safety Act amended PIPEDA was that they could not only use existing information that they held in order to share it, but they could collect further information at the behest of CSIS or the RCMP. They could seek out and gather it. They could be deputized, as it were, to go out to get more information, acting as agents for the RCMP.

This is what really concerns me. When you use the word “collect”, you have the right to collect further information. The private sector organizations that would be doing it are not subject to the charter rights, wherein everyone has the right to be secure against unreasonable search and seizure. It doesn't apply to a private organization acting on the request of the RCMP.

The chilling reality, as it strikes me, is that the information collection is without knowledge and consent. The individual might never know the fundamental rights to privacy the Supreme Court has established in its interpretation of the charter could be violated by a private sector organization. You would then have absolutely no right to redress, as you would if it were a public sector institution doing an end run on rights.

I think section 7 as amended by the Public Safety Act gives an end run to charter rights. It gives the RCMP and CSIS a mechanism to take an end run. Do you not agree that this invites a tremendous abuse of individual charter and privacy rights if it's a private sector organization at the request of an enforcement agency for sketchy reasons?

It's not only to stop a pedophile or some of the issues you cited. The reasons cited are for national security, the defence of Canada, which I think we can all agree would be laudable or worthwhile initiatives, or the conduct of international affairs. The conduct of international affairs is so wide and so abstract that it could mean almost anything.

Has this come up in the context of the RCMP? Have you contemplated the impact of the word “collect” rather than the word “use”?

● (0945)

Supt Earla-Kim McColl (Officer in Charge, National Child Exploitation Coordination Centre, Royal Canadian Mounted Police): If I may speak to our purpose in appearing before this committee today, PIPEDA has had an impact on our ability to do what we normally do on a daily basis, which is to go out to talk to people and ask them for basic information. The type of information we're talking about obtaining is less than what we get from running a driver's licence. We're talking about what I might get out of the phone book.

The amendments we're requesting to PIPEDA don't change that. It doesn't give us any additional powers. We're only seeking clarification. What we used to routinely go about getting on a daily basis when we talked to people on the street is all of a sudden unavailable to us because it's on the Internet.

Anything that invokes a charter protection is governed by the courts. They will ensure there is judicial oversight on any information we may obtain that is personal in nature. The amendment we're seeking is only to clarify the confusion that surrounds corporations.

Mr. Pat Martin: I understand that. I understand it, but I'm going beyond that. I have read your brief and I understand the amendments you're recommending here for those purposes, but it's the broader picture.

Currently, information can be shared under PIPEDA without the knowledge or consent of the individual in circumstances regarding a law being broken or those kinds of things. On this idea that the private organization will now not only be obligated to or will be allowed to share the information with the police, they could go out to gather and collect more.

Maybe you didn't realize that this extraordinary power seems to be vested now under the current PIPEDA.

A/Commr Bruce Rogerson: Under the present PIPEDA, the issue of lawful authority is the one that created confusion, by saying we needed search warrants or a court order in order to obtain information. It's one of our concerns.

We're not saying it's obligatory for anybody to give us information. It's clear and concise. When a police officer asks people for information—for industry, a certain customer's name and address information—we're not saying they're obligated. We'd like to think that as good corporate citizens, they would provide it. We're only saying it's permissible.

Mr. Pat Martin: This is about going further, though, sir.

Say you had reason to believe somebody was involved with gang activity, and my company held some information that would help you. You could also say to me, “Not only give me what you've got, but call that gang member up and try to suck him into revealing more information”—stuff you wouldn't be able to do without a warrant, or a search of his house.

Or let's say you're an insurance company, and the police might have reason to believe there's stolen property inside that house, but you can't get a warrant. The insurance agent, acting on your behalf, could go in and gather that information and then share it with you. The private sector is being deputized to do police work: that's what we read PIPEDA to be saying here.

A/Commr Bruce Rogerson: I think if we cross the line and say that we've now moved into an active investigation, then we start moving towards search warrants.

Mr. Pat Martin: Sometimes you say there's no time, in the case of a pedophile abusing a person online.

A/Commr Bruce Rogerson: But on a daily basis, I'll tell you that people give us information. You're right—we do seek more information from people on other issues, obviously, to get clarity and find out if in fact a certain activity is false or true before we move into the court-ordered stuff.

Mr. Pat Martin: But these aren't even crimes. What does the "conduct of international affairs" mean? It might mean a trade dispute.

A/Commr Bruce Rogerson: I will say that we've used our technology on two occasions to identify and pinpoint where hostages were within Iraq. We have used our technology to deal with major industries here in Canada.

As you know, one of the five priorities of the force—along with youth and aboriginal—is economic integrity. We do work with the industry to protect them. And we do work with them on an ongoing basis, whether it's a fishing scheme for the financial institutions—

Mr. Pat Martin: So that company could not only share personal information—

The Chair: Mr. Martin, your seven minutes is up.

Just before we go to Mr. Stanton, I want us all to be clear. You keep saying, "for the purposes for which we're appearing", so let's be clear on the purposes for which you're appearing today. That doesn't mean you can't answer questions on other things.

With respect to section 7, you're concerned that there's no definition of "lawful authority", and the ordinary service provider, in some cases, is interpreting that as meaning the requirement for a warrant.

You think that is incorrect and the act should be amended to clarify that. Is that correct?

● (0950)

A/Commr Bruce Rogerson: Yes, sir. What we're saying is that out of the 800 ISPs we have to date—and that industry is growing—

[*Translation*]

Mr. Robert Vincent: There's no more interpretation.

[*English*]

The Chair: Should I repeat it?

So as I understand it, your specific concern with section 7 is that the term "lawful authority" is not defined in the act. We heard earlier that as far as anybody knows, it hasn't been judicially defined or judicially interpreted, and that some providers, in particular Internet providers, may take the interpretation that "lawful authority" requires a search warrant. You believe that should not be the interpretation, and you're recommending to this committee that we recommend something to clarify that.

Do I have that correct? A yes or no would be fine.

A/Commr Bruce Rogerson: Yes.

The Chair: Thank you.

Now I have a question on section 9. If I call up my bank and say, "I'd like to know if the police have made any inquiries about my bank accounts", then as I understand section 9, the bank contacts you. They don't answer my question. They—or any police force—contact you, and they say, "My customer has asked if the police have inquired about his bank account. Is it all right to release the information?" Then under section 9, you decide whether or not there's an objection.

One of your problems is that's what happens if I ask. But my bank might choose to voluntarily call me and say, "Mr. Wappel, did you know that the police have been nosing around about your bank account?" Apparently, that is at least acceptable under the current interpretation of section 9, and you have a concern with that because you feel that if the police are inquiring before a client is advised of that action, the police should be given an opportunity to object to the client's knowing that.

That's the first part of your recommendations with respect to section 9. Is that correct?

A/Commr Bruce Rogerson: Yes.

The Chair: So what you're looking for is a ban on information being provided to the customer prior to consultation with the police forces. Is that correct?

A/Commr Bruce Rogerson: That is correct.

The Chair: The second portion, as I understand it, is that you want to have a blanket ability to object under all circumstances. Is that right?

A/Commr Bruce Rogerson: Yes.

The Chair: I'd like some explanation on that, but I'll let you think about that.

We'll go to Mr. Stanton.

Mr. Bruce Stanton (Simcoe North, CPC): Thank you, Mr. Chairman.

Just before I put my question, Mr. Martin cited some segments of PIPEDA. Could we get a reference to what section he was quoting from?

The Chair: Paragraph 7(3)(c.1), and then there are a couple of portions of that. There are different ways you can use lawful authority. One of them is what Mr. Martin cited, but there are others.

It's been indicated that the government agency asking for the information "suspects that the information relates to national security, the defence of Canada or the conduct of international affairs", but those aren't the only circumstances in which information can be asked for where lawful authority is cited without a search warrant.

Mr. Bruce Stanton: Okay. Thank you.

The Chair: Mr. Martin, did you want to jump in there?

Mr. Bruce Stanton: Well, this is my time, Mr. Chairman.

The Chair: I won't take your time away; let's just make sure we know what we're talking about.

Mr. Bruce Stanton: All right.

Mr. Pat Martin: Just to be accurate, and for the record, that was one of the clauses—thank you for knowing that, sir—but there's also subparagraph 7(3)(d)(ii).

The Chair: Okay, thank you.

Go ahead, Mr. Stanton.

Mr. Bruce Stanton: Thank you, Mr. Chairman.

Thank you to our witnesses for this morning's presentation.

Can you think of some other examples of legislation that you work with in the course of your duties that allow you to obtain personal information for the purposes of working on an investigation —specifically here, personal information, name, address, telephone number, identification information, but not sensitive information, if I can just set that aside—that is quite normal in the course of law enforcement activities?

● (0955)

A/Commr Bruce Rogerson: I can speak on that for a second.

On a day-to-day basis, dealing with the registry of motor vehicles and stuff like that, you get that on an immediate basis. The reality is that there's no other act other than—We use it in order to give us the empowerment to conduct the review or the investigation. It doesn't say anywhere in the act that people must comply.

In other enforcement areas, the Canada border security agencies, for for example, they have much stronger powers if they stop you at the border, but if we're acting in that capacity, at a border crossing or points of entry, then yes, it's compulsory to provide certain information.

Mr. Bruce Stanton: On that note, in the course of those types of investigations, presumably there are safeguards and practices for the use of that information, if it comes under the laws of evidence, or anything of that nature, that prevent it from becoming problematic vis-à-vis personal information becoming public knowledge. Correct?

A/Commr Bruce Rogerson: Yes, you're correct. Under the access to information, if people access stuff, it's vetted to make sure third parties are protected. No names are disclosed, it deals with the specific question of an individual without jeopardizing the rights and freedoms and privacies of other people. That stuff is vetted by several people within the RCMP. So in terms of that information, if any member of the general public wanted to access certain files, obviously it's vetted.

Mr. Bruce Stanton: Very good.

Supt Earla-Kim McColl: I would just add that certainly our authority's under the Criminal Code. We gather information about individuals under the provincial statutes, under municipal bylaws.

It's the nature of the work we do. We gather information about people and determine whether or not an investigation is warranted.

A/Commr Bruce Rogerson: And there's the proceeds of crime legislation, when they move forward to do a net worth or analyze the assets of an individual.

Supt Art Crockett: In addition, the national sex offender registry lays out specific points within there, that sex offenders are to provide specific information to police. And it governs, as well, how that information is to be collected, protected, and—

Mr. Bruce Stanton: I guess the point there is that there are numerous examples where laws and legislation exist that permit the use of personal information. In our case, this is what we're dealing with here under PIPEDA, for the purposes of investigating breaches of the laws of Canada.

My next question is in regard to section 7. We start in the preamble, really at the opening of section 7, specifically talking about the fact that an organization under subsection 7(3)—we discussed this a couple of times in various testimony and questions we've had at committee—"may" disclose personal information without knowledge or consent, etc., and then it cites the various conditions.

The debate has been on the question of the word "may", and the fact that nothing really obligates the organization. The question can be put but they really aren't obliged to provide under PIPEDA. It's their choice. In other words, the discretion is left with the organization.

Has that condition in PIPEDA been problematic for your investigations? Have you run up against organizations who recognize, for example, that you're a lawful authority, but they say the legislation only says they "may" disclose, so it's their choice if they wish to disclose or not?

Supt Earla-Kim McColl: That has been a great obstacle for us in investigating Internet-facilitated child exploitation. This is the number one issue for us, that interpretation of "lawful authority" and the interpretation of "may". It is being interpreted by service providers as permissive rather than optional. "May" was written to allow or encourage cooperation, but in fact it's being interpreted as though refusing to help is a viable option.

In our line of work, 35% to 40% of the requests that we make to Internet service providers are refused on the basis of PIPEDA. So we have some cases.... We have four recent cases in this country where getting us to the door, starting with a little bit of information from an Internet service provider, building upon it with a search warrant later on to get into the residence, has rescued four children. If we can't get this little bit of information we can't start an investigation and it leaves children at risk, and I think we're failing in our obligation to investigate these cases and try to rescue these children.

So it has had a huge impact for us. After consulting with the other OICs of vice units, I can say that this is the single largest impediment to our efforts today, this current legislation.

● (1000)

Mr. Bruce Stanton: Am I okay for time, Mr. Chairman?

The Chair: You have one minute.

Mr. Bruce Stanton: Thank you.

It would appear that even in the case of paragraph 7(3)(c), where you provide a warrant or a subpoena, the override still says "may". How do you get around that? Subsection 7(3) says, " an organization may disclose", and then paragraph 7(3)(c) says when it is "required to comply with a subpoena or warrant issued or an order made by a court", etc.

So that seems to be contradictory. Does that still work? If you produce a warrant, they still have—

A/Commr Bruce Rogerson: If we have a production order, or a warrant, or any other judicial authorization, then if they refuse we move through the judicial process.

Mr. Bruce Stanton: So the warrant will take out the questions around the word "may". Okay.

Supt Earla-Kim McColl: That section is not problematic. What we're talking about is information that is pre-warrant. We don't have enough to get a warrant, and that's why we use this section. But the "may" is problematic.

Mr. Bruce Stanton: Thank you for that clarification.

Thank you, Mr. Chair.

The Chair: Thank you, sir.

Mr. Dhaliwal again?

Mr. Sukh Dhaliwal: Oh, sure. Thanks. If nobody else wants to ask anything, I will certainly.

Thank you, Mr. Chair, again. My question is to our assistant commissioner, Mr. Rogerson.

You said to our chair that when the RCMP is investigating a person's bank account, the bank should be precluded from disclosing the investigation to this person. Should the RCMP also be precluded from disclosing this investigation to the public?

A/Commr Bruce Rogerson: We need to be consulted before they release the information to the individual on whom we're seeking information, because of the severity or level. And sometimes it heightens one's anxiety. Oftentimes we're working on just a tip, or there's a malicious person trying to implicate somebody in something that they're not doing.

We would like the people who are providing us with the information to consult with us before they release it so they understand the severity of it. It could be life threatening, in some cases, if they call somebody and say that we're looking, because the person would know that we received the name through somebody else. We may have somebody providing information who's embedded in an organized crime group, and if we call to validate, and a person finds out that we called to seek certain information, then that person will know that somebody gave us that name, and then you have an internal issue.

So yes, we would like to be consulted before one lets a member of the general public or an organization know that we're looking into personal information. Again, it's not that we have a criminal investigation going on. We're trying to gather information. It's just the beginning. We don't even know what we're growing and what we're looking into.

You must understand that as law enforcement officers, we set off trying to prove a person's innocence. Through that gamut, at the end of the day, we determine whether they're innocent or not. We don't go to work every day thinking we're going to put people in jail. We come to work not knowing what to expect. We receive information and we act on it, and we try to gather that information informally to determine whether there is an action, or in fact whether you even have to create an investigation.

With respect to what you're saying, I just go back. If we let people release information without consulting us, it could cause serious harm to individuals, and it also could cause serious harm to, let's say, an organized crime or terrorism file that we may be just starting to ramp up.

We use a certain methodology in the RCMP called a Sleipner model to determine whether it is an organized crime group or a terrorist group. That's information that is analyzed to determine whether it's good intelligence and whether there's sufficient grounds there to warrant a search warrant and move forward with a criminal offence or a criminal charge or a criminal investigation.

What we're really talking about here is just the first seed in the ground. We don't even know what the seed is. We don't know whether it's a flower or vegetable. When we do that, oftentimes we do it for the benefit of the public, and oftentimes they call us and ask if we've done anything with that.

The information we're talking about, remember, is the very basic information. It's at a very low level, but it could spur on, within a month, a very violent scenario.

● (1005)

Mr. Sukh Dhaliwal: That still didn't answer the second part of the question. So basically, you're telling me that you should also be precluded from getting that information out, then. That's the sense we got. On one hand, you are saying that banks should not disclose to this client that you are investigating and that you are asking questions. On the other hand, from the RCMP perspective, you should also not be disclosing that there is an investigation of this client going on.

Just a yes or no is fine.

A/Commr Bruce Rogerson: We shouldn't be disclosing it to anybody else.

Mr. Sukh Dhaliwal: It shouldn't be disclosed to the public.

A/Commr Bruce Rogerson: No. That's correct.

The Chair: You have five seconds.

Mr. Sukh Dhaliwal: Then, Mr. Chair, I'll go next time around.

The Chair: Thank you.

We'll go to Mr. Wallace.

Mr. Mike Wallace (Burlington, CPC): Thank you, Mr. Chairman.

I thank the panel for coming here today. Speaking for myself, I'm very proud of the RCMP and the work they do in this country, and I thank you for your service. My grandfather was an RCMP officer, and we're very proud of his service to Canada.

I hope you're not investigated, Mr. Martin.

Mr. Pat Martin: It wasn't me groaning.

Mr. Mike Wallace: Oh, I thought it was you.

Mr. Pat Martin: I didn't say a word.

Mr. Mike Wallace: There's one thing that's helpful for us as committee members to know when we're doing a review as we are today, not a line-by-line on a particular bill that's coming. Is there legislation, either provincially or in other jurisdictions, or any actual wording that you'd like to have or would like to suggest in terms of changes to the bill? We are meeting with the commissioner on Thursday, I believe, and that would be an opportunity for us to question the commissioner on some changes. Have you worked on actual wording, or are there other jurisdictions—

The Chair: We're having the Privacy Commissioner in, not the RCMP Commissioner.

Mr. Mike Wallace: That's right. Thank you, Tom, for pointing that out.

The question is, do you have actual wording that you'd like to see changed, in terms of suggestions?

Madam Earla-Kim McColl: I could make a suggestion. For paragraph 7(3)(c.1), the part with the "lawful authority" and the "may", we would ask that it stipulate that when a peace officer, acting in the scope of his or her duties, makes a request, that companies are authorized to provide it.

Mr. Mike Wallace: They would be authorized to provide it. That still does not require them to provide it.

Supt Earla-Kim McColl: That's correct.

Mr. Mike Wallace: Why is that an improvement?

Supt Earla-Kim McColl: It clarifies the "may". What it does is clarify for the companies that they're authorized to allow it, because that's the confusion that exists for them. Even for the companies that do cooperate with us—and many of them do—they're still not very comfortable about the ability to do so.

Mr. Mike Wallace: So for the 30% or 40% of Internet providers that have been reluctant to provide you with information, you believe that change in wording, the authorization, will give them greater comfort and give you a better position in terms of discussing with them the opportunities for them to give you the information.

Supt Earla-Kim McColl: We do.

A/Commr Bruce Rogerson: We want to take back the risk. The reality is that the way you've worded it, you've transferred the risk to them. In 30% to 40% of the cases, their legal advisers are telling them that they could be held out to dry if they give this information freely.

So we're not asking for an obligation, we're—

Mr. Mike Wallace: In terms of the 30% or 40% of ISP people who are not providing information, does the size of the organization matter? Is it the case that the larger the organization is, the more apt they are to cooperate?

● (1010)

Supt Earla-Kim McColl: That's correct. The larger organizations are generally cooperative. A significant number of small ones are also cooperative, but there are between 900 and 1,000 Internet service providers in this country. I will advise you that I haven't contacted all of them—we haven't had occasion to—but since we began taking statistics, I can say that 35% to 40% of them, on the basis of their legal counsel, have declined to cooperate with us.

Mr. Mike Wallace: That's in section 7, but you did have an issue with section 9.

Supt Earla-Kim McColl: Yes.

Mr. Mike Wallace: What's your wording for section 9?

Supt Earla-Kim McColl: Our wording for section 9 says, "a company shall not disclose any information regarding law enforcement interest without written approval (consent) of the investigator".

Mr. Mike Wallace: What's the change there?

Supt Earla-Kim McColl: The change is that they don't do it voluntarily, nor do they do it upon request of the client, without consulting with the investigator. If we are seeking that information to perhaps notify next of kin, there certainly wouldn't be any harm in letting the person know.

Mr. Mike Wallace: I'm going to give you my card. Could you e-mail those to me?

Supt Earla-Kim McColl: Certainly.

The Chair: You don't have to give her your card. I'll ask her to provide it to us.

Mr. Mike Wallace: Okay.

Do I have more time?

The Chair: Yes.

Mr. Mike Wallace: I'm going to share my time with Mr. Stanton. He wants to ask a question.

The Chair: You have time for one question, Mr. Stanton.

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

It's really a point of clarification, and I'll use this time if I can.

Going back to Mr. Martin's points that were being made, the reason I couldn't find the section was that I had the understanding that Mr. Martin was talking in terms of the availability of collecting this information under paragraph 7(3)(d), vis-à-vis foreign jurisdictions, national security, and international affairs. To be clear, that was all in the context of disclosure, not collecting.

In terms of collecting information, Mr. Martin talked in terms of how an organization can collect information, but paragraph 7(3)(d) doesn't pertain to collection. It pertains to disclosure only, so the information would have to be existing.

When we go to collection without consent, it's subsection 7(1) that applies. There's nothing in subsection 7(1) that suggests that the only reason you can collect it under subsection 7(1) is that it "is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws". So there are limits, and under the collection of personal information, there's a test that is contained in subsection 7(1) that would apply in those cases.

Thank you, Mr. Chair.

The Chair: All that may or may not be true, but I think this would be the subject matter for our in camera discussions, and not when we are talking with the witnesses.

I have two things. Before you leave today, would you be so kind as to provide the clerk of the committee with your recommended wording, so that we all have it exactly as you stated it?

A/Commr Bruce Rogerson: Yes.

The Chair: Also, did I understand your evidence, Superintendent McColl, that size does matter?

Supt Earla-Kim McColl: Sometimes it does.

Some hon. members: Oh, oh!

The Chair: Okay.

Monsieur Laforest.

[*Translation*]

Mr. Jean-Yves Laforest (Saint-Maurice—Champlain, BQ): Thank you, Mr. Chair.

Good morning to the three of you. Thank you for answering our questions.

I'd like you to explain to me something I had trouble understanding. On page 1 of your statement, you say that the introduction of PIPEDA has created some confusion, some uncertainty among the general public and that, as a result of that confusion, organizations are refusing to cooperate. Now I'm reading what appears near the bottom of page 3 of the English version:

> Section 7 was always meant to allow law enforcement to obtain personal, but not sensitive, information on a voluntary basis from companies on request. This is what we're seeking to restore.

When you say you're seeking to restore something that existed, that means there was good cooperation. So it's not necessarily just as a result of section 7 or the introduction of the act that there's now a problem. You say it worked well at first. You refer to section 7, among other things. Further on, you say that section 7 poses a problem, but you also consider it as the section that was used to enable law enforcement organizations to obtain information.

I find that somewhat contradictory.

A/Commr Bruce Rogerson: Not really. Most of the time we have good relations and good cooperation with contractors. However, as we say, there are still problems with 30% or 40% of them, who refuse to give us personal information because, according to their lawyers, it's really prohibited to give us that information. That's why we're here today, to find another wording, another way of clarifying the reasons why we need information. It's permissible, but because it's—

● (1015)

Mr. Jean-Yves Laforest: I don't understand why you say, on the one hand, that the same article was used to enable law enforcement agencies to obtain information and that you're seeking to restore that and, on the other hand, that the introduction of the act caused confusion. I find that contradictory.

[*English*]

Supt Earla-Kim McColl: I'm sorry, I'm not sure I understood the question well.

A/Commr Bruce Rogerson: The contradiction between our saying we have the excellent relationship in regard—

Okay, Art.

Supt Art Crockett: There are people who cooperate very well, and there are organizations that are very helpful. But we are finding more and more that companies get support from legal counsel, who generally want to advise their clients to be risk-averse. If it's not completely clear, their advice to their client would be that if there's a risk, and it says legal authority, then go get a warrant. Then you'll be covered; so don't release anything.

We're looking at the private sector and businesses who say, I'd like to give you this, but my counsel advises that I need a warrant.

So when we try to articulate our understanding that the act is actually enabling, they refer back to reduce the risk, and until it's clear, ask for a warrant.

In some cases, it's very good, we are happy, and it works. In others, it is not working. Our problem is that because it is not clear in all cases, there is a trend to move towards being more risk-averse and to release less information.

It was not our belief that PIPEDA was meant to do that. It was not meant to be a barrier to allowing communities to get involved, but in fact it was meant to be an enabler. So we are asking that the words be changed.

Where you might see a contradiction, it's not because it affects everyone the same—in some cases very well, in some cases no.

[*Translation*]

Mr. Jean-Yves Laforest: That's fine. Thank you.

[*English*]

The Chair: Mr. Stanton.

Mr. Bruce Stanton: I'm fine, Mr. Chair.

The Chair: Let's go to Mr. Van Kesteren.

Mr. Dave Van Kesteren (Chatham-Kent—Essex, CPC): Thank you, Mr. Chair.

I'd like to thank you all for appearing here.

I want to go back to service providers. Just out of curiosity, do they not want to give up information because certain providers may be known for that, and subsequently that's where you'll get the kiddie porn?

Supt Earla-Kim McColl: In some cases we believe that to be true, based on the fact they host websites that promote adult-child sex. We're never going to get 100%, but I believe this amendment would increase our ratio to 80% or 90%. It would give them the comfort so they could share information with us.

Mr. Dave Van Kesteren: Aren't there laws in place for compliance? Even if you are not responsible for the crime, if you've helped in another way aren't there laws in place for—

Supt Art Crockett: It would be for harbouring a crime, or being party to an offence.

Mr. Dave Van Kesteren: That's the one.

Supt Art Crockett: Yes, there are; however, we are in the very early stages and we have yet to determine that there is a crime. At the point when we know a crime has been committed and who the parties are, we won't be asking subtle questions; we will be seeking the authority and support of the court to obtain that information. It is in the very early stages that we're talking about.

Mr. Dave Van Kesteren: The current act has been criticized for not having any teeth. Presently, upon investigating, the commissioner may publicly expose companies that have breached the act. That's basically the deterrent we have.

Does the act allow for the same action by the commissioner for the police? If it doesn't, should it? In other words, if the police, like any corporation, were to breach the act, the letter or intent of the law, does the Privacy Commissioner have the power to publicly chastise the police?

● (1020)

A/Commr Bruce Rogerson: Yes, and I'll talk about the Public Complaints Commission because that's the number one watchdog.

As you know, with the recent O'Connor report and stuff like that, in the near future the RCMP will have an oversight committee and a governance structure. Throughout Canada your municipal boards, police boards, and committees can take action long before it gets to the Privacy Commissioner if somebody misuses the information.

I often think we're the defenders of human rights and protect basic privileges. Along with all that oversight are the number of regulations we fall within that allow us to take immediate action against anybody who violates the trust we have been given through PIPEDA, and ask for that information. If that information is not in line with the execution of their duties, a number of regulations and guidelines allow us to discipline an individual for outright breach and, depending on the severity of what they exchanged, determine the level of sanction against the individual.

Under our new commissioner, the direction to the Privacy Commissioner on public complaints is that our books are open. They can have access to see if there's any abuse. The Auditor General, who has been in to our organization on numerous occasions, represents the best interests of Canadians as a whole. She has never identified that we've misused this type of information.

So in light of what you've asked, the answer is yes.

Mr. Dave Van Kesteren: Mr. Crockett, if you're party to a crime—and I know this doesn't deal with the Privacy Commissioner or the Privacy Act—can the service provider be charged if they have provided service to somebody that's—?

Supt Art Crockett: Yes. Under the Criminal Code a person can be held accountable for actions in which they have aided in a criminal offence. If they are party to an offence they can be held accountable.

Mr. Dave Van Kesteren: Thank you.

The Chair: Mr. Martin.

Mr. Pat Martin: Thank you, Mr. Chairman.

Let me just start by saying that I do understand the point you've raised, and I do have some sympathy for the points you've raised, especially in the identification of pedophiles, etc. I'm trying to go beyond that, though, to explore what PIPEDA means to the RCMP in the context of, let's say, terrorist investigations, where it may be CSIS or the RCMP.

Under PIPEDA—and Mr. Stanton is correct in the chapter and verse that he cited—information collected by a private sector organization in secret, and without any constraints other than that the organization has suspicion that something is going on, that information could well be handed over to the RCMP and form the basis of a charge. Wouldn't that fit under the rubric of tainted evidence, if the information was garnered in a way that violated the individual's expectation of privacy, because he had a relationship with that company, maybe even a contractual relationship that guaranteed him the right to privacy that information wouldn't be used?

To me it opens the door, because private sector organizations don't operate under the same legal obligations as law enforcement and national security. You would have to have reasonable grounds to suspect something illegal was going on. They—the language used here—are “suspect”. So if your boss has a suspicion that you have something in your locker, that's all he needs to go on. You need something greater than that, reasonable grounds. I think that it's a slippery slope to tainted evidence, leading to possibly righteous convictions, but from a tainted evidence source.

Supt Earla-Kim McColl: It depends on how the investigation commences. If they're acting on the direction of the police, then they're an agent of the state, and there are considerable checks and balances involved. If they're doing it on their own and then they hand it over, then our involvement starts when they hand it to us.

● (1025)

Mr. Pat Martin: That's exactly what the change to the Public Safety Act dictates, that they can collect this information at your request, which is one thing, but would have some controls, or the organization may now collect information on its own initiative and then make subsequent disclosures under PIPEDA. Even though PIPEDA binds them to keep your information sacred as its primary obligation, it also may hand that information over to you, which may result in a charge and a deportation to a country, because they suspect some Muslim guy is a terrorist because of what he said in the lunchroom.

Supt Art Crockett: Any and all evidence that is collected in any type of investigation, if it goes before the court will be judged on its merit, and the protections that fall within—

Mr. Pat Martin: But what used to be tainted evidence is now okay, because of PIPEDA.

Supt Art Crockett: PIPEDA protects the person who shares the information with the police. The police will still be accountable for the evidence they obtained and how that evidence was obtained. The court will still hold the Crown accountable for the evidence itself.

Mr. Pat Martin: But the gathering of it, they're not bound by the same rules of gathering evidence, etc. A private organization, if operating on its own initiative, doesn't have any of the constraints that a law enforcement agency has.

Supt Art Crockett: But the evidence will still be—

The Chair: Excuse me, Mr. Martin. Could you refer us to the exact section that you're referring to, please?

Mr. Pat Martin: I apologize, I didn't bring all of my files. I'll bring it to the—

The Chair: As you're asking the questions, I'm trying to find in my copy of the act the specific wording that you're looking for, and I can't find it. Now, that's not to say it isn't there, I just can't find it. I'm a little hesitant to have the witnesses answer questions based on your interpretation of a section if we can't have it in front of us to take a look at what the actual wording is.

That's no disrespect to your recollection, but I can't find it.

Mr. Pat Martin: I understand, although I do sense we're getting some agreement from the RCMP that this is the way they understand PIPEDA as well.

The Chair: Okay. Good.

Mr. Pat Martin: They could either ask a private sector organization to collect information, or the private sector organization may collect information on their own and divulge it to the RCMP.

A/Commr Bruce Rogerson: From our point of view, we determine whether it's evidence or not.

We have collaborations, obviously, with the hydro sector and other major infrastructure industries that have internal corporate security. Yes, if we identify a person who has a certain affiliation with a certain group, we alert them to let them know that they should keep an eye on that individual. They may in fact work on our advice to them.

In this private-public partnership that government is trying to drive—and we're at the table all the time—as one of the concerns they have the private sector people say, “We have all this to offer, and what can you offer us?”

Going back to the original concern, we say it deals with what level of security people have within each industry. Do they meet our top secret—? Can they be held accountable under the secret offences act? That determines how close our interoperability is.

For our part, either we can alert them as to an internal operative who could bring down Hydro Ontario by throwing one switch; or they might say, we're highly suspicious of this individual, who seems to be accessing files within our system that really have nothing to do with their job. So they may gather information, but when it reaches us, we look at it, and that step becomes the footings for us now to ask whether this is an investigative time, whether this is evidence.

The crown prosecutor or the Department of Justice will look at it and weigh whether or not it's admissible or inadmissible, and we flow from that.

But yes, you're correct. If I were an investigator and knew somebody who was working on a bridge and who might want to blow up the bridge between Detroit and Windsor, I would certainly let Transport Canada know—for instance, I'd like you to keep an eye on that person, because they're affiliated with certain groups. Then they would start gathering information for their self-protection.

In the old days, we wouldn't tell the bank the robbers were coming. So the robber would come, go into the bank, put everybody at risk, and leave. Then we'd arrest him outside the door and say, there, we caught you robbing the bank. Now what we do is call the bank to let them know there's a possible—

Mr. Pat Martin: This guy looks like he might be a bank robber: arrest him.

A/Commr Bruce Rogerson: No, it's that this person is coming, and we have all the evidence we need that they've conspired to commit a crime—

● (1030)

Mr. Pat Martin: Except now we have a private sector organization being deputized to make those same judgments. The RCMP, I trust, has the expertise to make those judgments. I'm not sure the private sector guy does, especially when he has an obligation to keep the privacy of that individual paramount.

If PIPEDA is all about protecting individuals' privacy, we've left a loophole in it big enough to drive a truck through. No one's privacy is paramount, because under these sections, which I will refer you to if I get the numbers straight, as we read them, any private sector organization can blow your privacy out of the water on a mere suspicion that you may be up to something, and under very vague categories—not only national security, but international....

What is the term they use? Oh yes, it's the “conduct of international affairs”.

The Chair: Mr. Martin, because I interrupted you, I gave you seven minutes in a five-minute round, so you're over. I'm not necessarily sure I subscribe to your interpretation, but we'll see when we look at the act.

I'd like to go back to the witnesses for my purposes on section 9 again. Section 9 has certain grounds listed upon which you can object to the fact that you're investigating someone, or inquiring about someone, being given to them. I just want to be clear, based on your testimony, that you're not suggesting those grounds be somehow taken out or anything, that you're comfortable with those grounds upon which you can object.

So when you say that section 9 should be clarified to ensure the police can object to the disclosure of information provided to law enforcement in all circumstances—Well, you can do that now, can't you?

Supt Art Crockett: Right now it is not widespread, but there are a number of groups or individuals who feel that this disclosure does not take into account should they choose—

The Chair: No, I understand that point.

If Tom Wappel inquires from his bank, the bank must notify you, and you have certain grounds upon which you can object to that information, and that's the end of it. And you're happy with that.

Your concern is with the bank, on its own, contacting me without previously contacting you and saying that the police are investigating. You want to be able to have those same objection abilities when the provider decides to give the information. Or you might ask that the provider in all cases not be allowed to give the information unless the client asks. Are you asking that?

Supt Art Crockett: Unless they confirm with the police that they are able to release the information; we won't know at the time whether or not it can cause harm, but we will know when they call.

So provided they contact us, we don't have an issue. It is when people feel they can find a loophole by interpreting it to mean, "I know I can't release it if they ask me, but I can choose to release it on my own; therefore, I am covered."

The Chair: Got it. That's good. Thank you; I understand the point.

We will go to Mr. Dhaliwal again.

Mr. Sukh Dhaliwal: Thank you, Mr. Chair.

I will return to where I left my question last time, and back to the assistant commissioner. This is a real-time example with fictitious names, and it is a very recent example.

Let's say Dow Jones's spouse got murdered, and Income Trust is a friend of this Dow Jones. An RCMP officer picks up a phone and goes to the white pages of the book. The RCMP officer picks up the phone, calls the Income Trust person, tells Income Trust that they are doing an investigation against Dow Jones, says that a murder has happened, and asks if Income Trust is friends with that person. The way I look at it is this. You said you should not be disclosing it, and that if it's disclosed it can jeopardize the investigation totally. Even though that Income Trust is not the right person, this RCMP officer just went to the white pages, and he was calling every Income Trust listed in the phone book.

The way I look at it is if this Income Trust person who was called by the RCMP goes out and tells Dow Jones that there is an investigation going on, and that they are looking for a person named Income Trust who is a friend with you, I think it is going to jeopardize the whole thing. On one side this could really be the person in that particular murder, but on the other hand if those are innocent, it can jeopardize the integrity of those two people as well.

Would you like to comment on that, under this act?

● (1035)

A/Commr Bruce Rogerson: When you said you went through the white pages, obviously that's the reason to go PIPEDA; you're looking for a needle in a haystack. You don't know where the information is. In that instance, you are saying, they may have discredited the individual's name inappropriately, yet at the end of the day the change, as I said before, is that we are willing to accept that risk, and if we do cause undue harm to an individual, obviously we are held accountable for it.

Is that what you are seeking?

Mr. Sukh Dhaliwal: No, I'm seeking from the victim's point of view as well, the victim who died. This individual the RCMP officer called is not the right individual. It's a small community, and this person goes to the suspected person and tells them that the RCMP is looking for them. I think it's already jeopardizing, because the way I was coming is that you said you should not be disclosing that investigation at all, and this RCMP officer has already disclosed that.

A/Commr Bruce Rogerson: Given your scenario, I would need, as a previous investigator in my young life, a little more information to appropriately—

Mr. Sukh Dhaliwal: This is a real-time example, so I can't go further. I gave you enough there. I think you should be able to go back to the question that I asked earlier.

You said you should not be disclosing that there is an investigation going on against a certain person, right? On the other hand, I see that in real time it is happening, even at this point in time.

Supt Earla-Kim McColl: The important distinction to make is that we are seeking the truth. We go out and ask questions, but we also are governed by privacy rules and regulations. We disclose as little information as possible in order to seek the truth by asking questions. If there is an inadvertent impression left with people we speak to, that's unfortunate, but what we do is go out and ask questions and try to find out the truth.

Mr. Sukh Dhaliwal: This officer mentioned specifically that they were doing a murder investigation into this particular case, into the Dow Jones case, and that they were looking for the Income Trusts who were friends with Dow Jones. That is very serious to me. It seems like this officer has gone way too far to jeopardize the investigation itself, and also, if those two people are found innocent, to ruin their reputation as well. It's both ways. I don't see—

When I asked the assistant commissioner earlier, the assistant commissioner said that you should not be disclosing that investigation, and it's already done. It's a real-time—I can give you the names later on, if you want.

Supt Earla-Kim McColl: I think I know the case that you're referring to.

A/Commr Bruce Rogerson: If what you're saying is true and the person was not acting within lawful authority and put the case or the investigation at risk, along with the livelihoods of innocent individuals, then they would go through our internal complaints unit, which functions fairly well and in some cases extremely well. If they're not satisfied with that outcome, they would then go through the Public Complaints Commission to get a secondary review.

I can't qualify every case. If you have a trusted relationship with a certain industry and their security people have the right security clearances and can be held accountable, in order to then justify the rationale for asking for the information, sometimes I'm sure the police officer may explain it in a fashion that might or might not put somebody in jeopardy.

I'd have to review the facts in this case. If you're saying a murder investigation was being conducted and the individual was told that's why you were doing it, I'd have to look at the information that was disclosed to rationalize a qualified response to your question.

In the course of their duties, most members might walk around the neighbourhood. As Superintendent Crockett mentioned earlier, if there's a murder and you don't walk around, you don't have any witnesses. So you go around and ask if they've seen anybody, because there's been a murder next door. You explain to people why you're seeking the information. You ask questions. Did you see anybody suspicious? Did you see anybody coming in and out of the house? Did you see a car? Did you take the plate number? Do you know the make and model?

So when you move in that type of scenario, it does two things—

● (1040)

Mr. Sukh Dhaliwal: But Assistant Commissioner—

The Chair: I'm sorry, you're way beyond your time, Mr. Dhaliwal.

I think what Mr. Dhaliwal was saying is this. It would be if an RCMP officer went to next door neighbours and asked if they happened to know where Tom Wappel was because the officer thinks he committed the murder, as opposed to asking if they happened to know where Mr. Wappel was—the implication being that the guy who's been accused by the investigating officer may perhaps be exonerated later on.

Is that the general drift of what you're talking about?

Mr. Sukh Dhaliwal: Mr. Chair, it's also jeopardizing the victim as well, the victim who died. You mentioned your name. Now we know that the RCMP officer is looking for Tom Wappel, who is involved in this. It's not going to the real Tom Wappel, it's going to the wrong Tom Wappel. The wrong Tom Wappel now goes to the real Tom Wappel and tells him that the RCMP is investigating. They can hide that information as well.

So I'm coming from both sides.

The Chair: All right. I think one Tom Wappel is enough.

Monsieur Vincent, s'il vous plaît.

[*Translation*]

Mr. Robert Vincent: Thank you.

Does your service investigate any type of fraud? Does it investigate fraud?

A/Commr Bruce Rogerson: Yes.

Mr. Robert Vincent: Does it investigate fraud relating to identify theft?

A/Commr Bruce Rogerson: Yes.

Mr. Robert Vincent: Yes?

A/Commr Bruce Rogerson: Absolutely.

Mr. Robert Vincent: Can you tell us the approximate number of identity thefts that can be handled, of cases where someone used another person's identity to rob, obtain a line of credit at a bank or anything else? Do you regularly investigate those kinds of cases?

A/Commr Bruce Rogerson: Yes.

Mr. Robert Vincent: So you're aware that it's appropriate to give certain persons more independence. We've also observed that the insurance companies want a power to investigate other insurance companies to check whether there has been an accident or a car theft involving another insurance company.

Everyone who comes here wants an expanded power of investigation to obtain personal information on everyone. The problem is that, if you telephone a given person to obtain information in the course of an investigation, how can that person at the other end of the line know who he's giving that information to? Even if you are a police officer! How can that person determine that?

For example, you introduce yourself as Officer Crockett, and you say you'd like to have some information on a particular person. You demand that information because the act permits you to obtain it. Is that how you proceed?

A/Commr Bruce Rogerson: By telephone?

Mr. Robert Vincent: Yes.

Mr. Bruce Rogerson: I don't think so.

Mr. Robert Vincent: Earlier, in response to a question, you said that you made telephone calls, that you gathered information by telephone and that you conducted your investigation by telephone. That's what you said earlier in response to Mr. Dhaliwal.

[*English*]

Supt Art Crockett: It's very difficult for us to speak about a specific investigation if we have not done the background to determine exactly what phone calls were made.

Mr. Dhaliwal initially provided a set of circumstances, which we are trying to interpret, but it would be a lot easier for us to be able to fully respond were we to know the investigation.

To answer your question, sir, in generality—

[*Translation*]

Mr. Robert Vincent: Let's take the example of what happened in St. Thomas, Ontario, and of the investigation conducted over the Internet. Do you call the distributor to determine which people subscribe to Internet service?

[*English*]

Supt Art Crockett: If you're seeking information specifically with individuals, we will do that in a face-to-face.

If you have a rapport with the company, they know who you are, and they recognize your voice, it may be possible to do that by telephone.

Yes, I would expect the company would ask how they know it is us—i.e., how do I know you are police; can I call you back at the police station and receive you on the other end? There are always ways to be able to do it.

We as an organization and as a law enforcement community are the last line of defence for the privacy of individuals. We guard that information closely. It is never our intention to harm someone by going through that. But we appreciate your point.

● (1045)

[*Translation*]

Mr. Robert Vincent: I can understand. I don't doubt your integrity, but criminals don't have any integrity. They can impersonate you three and obtain personal information from anyone simply because the act enables them to do so.

Tomorrow morning, I could get a card from the RCMP with my name on it. I could then go and see someone and tell him that, under section 7 of the act, I'm entitled to ask him for this information. Then I would have information on Mr. Rogerson in hand. I could know how much money he has in his bank account. If that amount were in six figures, I'd only have to go to another bank to apply for a line of credit, and that would be it! I would have withdrawn $25,000 or $50,000 from the bank after stealing his identity thanks to a business card, all in the space of an hour.

I could take one of your business cards and go to any merchant and tell him that the act allows the identities of these people to be revealed.

What do you do in those cases?

[*English*]

Supt Art Crockett: Clearly, they—

[*Translation*]

Mr. Bruce Rogerson: Relations between police officers and the institution are often good.

Mr. Robert Vincent: What happens if no one in that institution knows you? I could go to the corner convenience store and ask for a copy of all the transactions conducted between the convenience store and that man because he uses his credit card or debit card every day. Today I'm targeting him. I know his address, and I want to get more information on him. I have his business card and I ask for personal information about him. The act permits that. I take a copy of section 7, and I tell them that, under that section, they have to give me that information. The person there trusts in the business card.

[*English*]

Supt Earla-Kim McColl: I've think you've hit on the important portion we're trying to remedy today, and that is the question of lawful authority.

When we deal with companies, we provide them with a facsimile with our letterhead on it and a supervisor's name. Or we have a personal relationship with them so that I can phone and say, “Hi, it's Earla-Kim.” However, we encourage people when dealing with law enforcement officers to be sure of who they're talking to. People will impersonate us. Certainly we ask them to check identity and be certain about who they're speaking with.

[*Translation*]

Mr. Robert Vincent: You understand that I can obtain a letter like that in two minutes. I only have to go to the RCMP Web site, copy the logo, print it, write what I want in the letter, sign using any name or that of an RCMP commissioner, and that's it. I only need two seconds. Section 7 makes it possible to tell people that the act provides authorization to give out personal information.

[*English*]

Supt Earla-Kim McColl: Again, the distinction is important. What we're asking for is not considered protected or personal information. It's tombstone data. These are things like a name or an address, which I can get by talking to your neighbours. I can drive by your house and then go to city hall and find out your name and address, how much you paid for it, and how much you owe on it.

What we're looking for from our partners, in our effort to keep our community safe, is minimal information, which we've always been able to get just by talking to people. PIPEDA has made that more complicated for us. We're trying to get back to that level playing ground. If the information is considered personal or protected or in any way confidential, then we're governed by the charter. We're governed by all the checks and balances that the courts give us.

This is not about giving us new powers. This is about getting us back to where we were.

The Chair: Thank you.

I gave you seven minutes, Monsieur Vincent.

I have nobody else on my list. If nobody wants to ask anything, then we'll go back to Mr. Vincent.

Mr. Martin.

Mr. Pat Martin: Thank you for the opportunity.

I hope you don't feel that we're deviating wildly from the reason you came here. I think we do accept the legitimate points you've made in your brief about section 7 and section 9. But having officials from the RCMP here, and given the nature of the material we're dealing with, we can't help but explore other issues.

One issue is that tomorrow we will vote on a new bill that we argue creates an identity theft kit for all Canadians to use. The Government of Canada will now put your date of birth on the permanent voters list. You will have name, address, telephone number, and date of birth.

Does this raise any concerns for you? Do you share our concern that the date of birth is a piece of personal information, which is sometimes used as a PIN? It's your identity. We think this is a formula for identity theft that could exacerbate the existing problem.

● (1050)

Supt Earla-Kim McColl: The courts don't generally consider that type of information as personal, and we certainly discourage people from using a DOB as a PIN number. DOBs are not considered personal, private, confidential pieces of information. Those are things that are available.

PIPEDA isn't about protecting information. It's about how we use it and disclose it. I know I applied for a credit card, and I now get a raft of stuff in the mail. Somebody is certainly disclosing that, but I trust that it's being disclosed in accordance with those guidelines.

Mr. Pat Martin: But when you phone up that credit card company to say you'd like to activate this credit card they so generously sent you in the mail, quite often they'll say that to make sure it's you, they need your date of birth. You say, December 13, 1955, and then they know it's really Pat Martin.

We're very concerned that this is going to be abused. At least in the short term, it's going to create a rash of activity in this regard with this new information that's now in the hands—

We're just about to go into a federal election, so we now have this new law, with a new voters list. I had 250-some—

The Chair: Mr. Martin, I'm sorry to interrupt you, but can we make this relevant to PIPEDA? This is a review of PIPEDA. This isn't estimates or anything like that. We're reviewing PIPEDA, and I can't see how this new act that we're about to vote on, about elections, has anything to do with PIPEDA.

Mr. Pat Martin: Let me explain.

Actually, PIPEDA is about protecting personal information. It's right in the name of the act. Every riding association is now going to set up a campaign office for every political party, and they're going to have the permanent voters list laying around. Under PIPEDA, there's an obligation that any institution, agency, or organization under federal jurisdiction has to abide by PIPEDA to protect your personal information.

Is it your feeling that your date of birth is not personal information that warrants protection in light of this widespread electronic identity theft that we're facing?

A/Commr Bruce Rogerson: The courts have ruled that it's not protected information under the charter. What you're arguing against is the idea that they're saying it's normal data available to other people through other venues and everything else. It's up to somebody else as to how you address PIPEDA in terms of how they disseminate the dates of birth.

Obviously, a gentleman earlier talked about identity theft and stuff like that, and yes, there are issues around that. For what we ask for through PIPEDA, though, the court has ruled that it does not violate the charter. It's admissible evidence. It's admissible information. It goes right down to what you say, including tombstone data and their dates of birth.

I'll leave you with these three decisions if you want, from the previous—

Mr. Pat Martin: It would be helpful if they could be tabled for circulation.

The Chair: Could you leave those with the clerk, please?

Mr. Pat Martin: My last point on this is simply that the Office of the Privacy Commissioner agrees. We have a letter from her, as of Monday of this week, accepting our complaint regarding the distribution of dates of birth on the permanent voters list. She is agreeing that it is a serious concern. I just wanted your views on it, and I thank you for that.

A/Commr Bruce Rogerson: Just to extend on your point, we've noticed under the firearms registry that even by giving three letters of a postal code, people can zero in on where firearms are, and then we see heightened activity around break-and-enters into various homes.

So we're not the only analysts in the world. Criminals and organized criminals out there now have their own analysts. It's up to you to decide whether or not they can use those pieces of information to not only get your date of birth, but information on whether you own a gun or whatever else.

We share similar concerns, because we're about prevention. If we can prevent something, then we're all for it, especially if it's an act.

The Chair: Thank you.

We have five minutes. We'll give two and a half minutes to Monsieur Vincent and two and a half minutes to Mr. Stanton, and then we adjourn.

Monsieur Vincent.

[*Translation*]

Mr. Robert Vincent: Thank you.

I'd like to finish the story that I started earlier because it's a bit disturbing. I'm still afraid because identity theft is the most common thing these days. It's the most widespread type of fraud for which there are the fewest convictions, because it's hard to trace a person or someone who has used the name of another person. Stealing money is so easy and so quick! You know that all the people who want to break the law are on the look-out for all the new acts and everything that happens in the courts so they can be more up-to-date than the police.

Since, from one day to the next, these people could know that section 7 of the Personal Information Protection and Electronic Documents Act has been amended, giving police officers the opportunity to access all information allowed by occupation, aren't you afraid that someone may steal your identity and use it to obtain others in order to commit theft or something else? Haven't you thought that that kind of thing could happen?

● (1055)

[*English*]

Supt Art Crockett: Sir, is your question whether or not we feel there would be a threat if information were given to police, that it would be stolen from us? Do you feel that we will not secure the evidence?

[*Translation*]

Mr. Robert Vincent: No, imagine that I use your name tomorrow, Mr. Crockett, that I take your business card and go to the corner store and tell them that I'm conducting an investigation — my letter confirms it — and I ask them to give me personal information on a person, his social insurance number and so on. Is that possible?

Mr. Bruce Rogerson: Every person has the right to phone the police station and check.

Mr. Robert Vincent: Suppose I have your business card and a letter from the RCMP confirming that I'm conducting an investigation. I present it to the person opposite me and I tell him that it isn't necessary to call. I'm there and I'm requesting personal information on someone. Does section 7 of the act, which gives me the power to ask you for that information, make that possible?

A/Commr Bruce Rogerson: In your view, it's—

[*English*]

Mr. Robert Vincent: Your speaking in English is not a problem.

[*Translation*]

Mr. Bruce Rogerson: No, everybody has the right to give us the information, but it's not mandatory.

Mr. Robert Vincent: You're not answering my question.

[*English*]

The Chair: Mr. Vincent, you got an answer. That's your time.

Certainly, if somebody impersonates a police officer, you can't expect the *dépanneur* not to answer the question, obviously.

Mr. Stanton.

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

I wonder if I could use this occasion with our esteemed panel here today to say that we have a motion in front of the House right now concerning the Anti-terrorism Act. I wonder if you'd have any thoughts on what Parliament should consider in respect to the Anti-terrorism Act—in fact, the two considerations that we're considering renewing for a period of three years.

The Chair: Mr. Stanton, that's a good question, but how's that relevant to PIPEDA?

Mr. Bruce Stanton: I thought I'd try, Mr. Chair.

The Chair: It's a good try, but I really don't think it's relevant to PIPEDA.

Officers, thank you very much for your appearance today. We do appreciate it. I'm surprised we went the full time, but I guess when the RCMP is here there's room for all kinds of questions on all kinds of things, as you heard. So many thanks again for your evidence. Please be sure to give us the three cases that you mentioned, and the specific wording of the amendments that you would like.

I adjourn the meeting until Thursday, when we will have the Privacy Commissioner before us, and hopefully we'll have some very pointed questions for her about some of the recommendations that have been made to us.

Thank you.

Published under the authority of the Speaker of the House of Commons

Publié en conformité de l'autorité du Président de la Chambre des communes

Also available on the Parliament of Canada Web Site at the following address:
Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante :
http://www.parl.gc.ca
