House of Commons
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 030 • 1st SESSION • 39th PARLIAMENT

EVIDENCE

Tuesday, February 13, 2007

Chair

Mr. Tom Wappel

Also available on the Parliament of Canada Web Site at the following address:

http://www.parl.gc.ca

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, February 13, 2007

● (0900)

[*English*]

The Chair (Mr. Tom Wappel (Scarborough Southwest, Lib.)): Good morning, everyone. It's a nice cold morning.

I call—

Mr. David Tilson (Dufferin—Caledon, CPC): Mr. Chairman, while you're getting your breath, I wonder if I could have a point of order.

The Chair: Sure. Go ahead.

Mr. David Tilson: As the vice-chairman, I'd like to say that most members, if not all, have read the obituary about the passing of your mother. Obviously she thought a lot of her family, and you and your family thought a lot of her. We offer our condolences.

The Chair: Thank you very much. I very much appreciate it. And yes, we did think a lot of her. She was a wonderful person.

Today we have, from the Canadian Resource Centre for Victims of Crime, Steve Sullivan. Hi Steve.

We also have Krista Gray-Donald, director of research. Good morning.

From the Insurance Brokers Association of Canada, we have Robert Kimball, chairman; Peter Fredericks, vice-president; and Steve Masnyk, manager of communications. I'd like to thank the insurance brokers for sending around the blanket once in a while to the MPs. I appreciate it.

From the Canadian Association of Chiefs of Police, we have Clayton J.D. Pecknold, co-chair, law amendments committee.

Welcome to everybody.

I guess we'll start in the order the witnesses are listed and ask Mr. Sullivan to make his opening remarks.

By the way, as everybody knows, you have up to 10 minutes to make your remarks—we do time you—and then there will be questions from the members. So don't worry, if you happen to run over, anything you don't get an opportunity to say in your remarks I'm sure you can say in your response to questions.

Go ahead, Mr. Sullivan.

Mr. Steve Sullivan (President, Canadian Resource Centre for Victims of Crime): Thank you, Mr. Chair, committee, for allowing us to come today to talk about issues related to your review of PIPEDA. I don't think we'll be very long in our opening remarks. Our issues are pretty specific. We just really want to raise those for you, and we'll be happy to try to answer any questions.

Very briefly, the Canadian Resource Centre for Victims of Crime is a national non-profit advocacy group for victims. We work with victims from across the country in providing direct advocacy services. We also try to raise issues with all levels of government, advocate on behalf of victims to promote their rights and their interests, and promote laws to better protect them. It's that latter role that I'm here in today, to try to promote some amendments and raise some awareness on issues that we think require some attention to better protect children, in this case, from Internet child sexual exploitation.

I should mention that we are funded by the Canadian Police Association. We have been sponsored by the police association since 1993, so we have had a lot of interaction with various law enforcement officers across the country. Some of those are investigators who work directly with these issues.

Contrary to a lot of public opinion, I think what law enforcement unfortunately faces on a day-to-day basis in dealing with these issues is not children frolicking on beaches or pictures of kids running around in their underwear; it is the rape and torture of children, sometimes babies, by men, and often their fathers or uncles. Those images are kept and put on the Internet for anyone and everyone to see. They are traded like baseball cards. There are thousands of images of children all around the world. Last week, we saw a huge bust resulting from Australia that has had impacts in many countries, Canada included.

One of the issues we want to speak to today is what the impact of PIPEDA is on law enforcement's efforts to try to address these issues. In our interaction with the members of the Canadian Police Association that we deal with from time to time, and also in following media reports, it seems there is some confusion with regard to the PIPEDA legislation and whether or not Internet service providers can or should provide information to law enforcement regarding subscriber information, like people's names and addresses. It's our position, very succinctly, that ISPs should frankly not have discretion to share that information with law enforcement efforts. At the very least, with this legislation, we need to make it clear that ISPs can and should share information.

We have provided a brief. I apologize for not getting it to you sooner so that it could be translated, but we have left copies with the clerk.

The issue of child pornography has been raised in various committees over the last couple of years. We sent a brief to all members of Parliament six or seven years ago about child pornography, along with some recommendations that we had made at that time. Some of them have been implemented, like the creation of a luring offence and the creation of a national tip line, which is now in operation and had I think 6,000 tips in the first year of operations alone.

Various other committees have heard from experts who have far more expertise in this area than us. I just want to read a very quick quote from OPP Detective Inspector Angie Howe, who spoke to a Senate committee in 2005 on Bill C-2, which had a variety of different measures, some of them regarding child pornography. What she said then was:

> The images are getting more violent and the children in the photos are getting younger. As recently as one year ago, we did not often see pictures with babies, where now it is normal to see babies in many collections that we find. There is even a highly sought-after series on the Internet of a newborn baby being violated. She still has her umbilical cord attached; she is that young.

I say that not to shock you or disgust you—although I suspect you are disgusted—but just to really get the message across of what it is law enforcement is fighting.

In our efforts to raise these issues, we have heard of the notion of Big Brother and that law enforcement wants access to all this information. What they're doing every single day is sitting in front of a computer, sifting through tens of thousand of images. One accused person could have 10,000 images of children being raped and tortured. That's what law enforcement is dealing with, and those are the children we come here today to try to speak for.

You're dealing with PIPEDA, which is an act relating to privacy. Can you imagine any greater violation of your privacy than having the most awful images of you captured for anyone and everyone to see? Unfortunately, no one is speaking for those children. No one is talking about their privacy rights.

● (0905)

We have a Privacy Commissioner who I'm sure does an absolutely fabulous job on a variety of issues, but as far as I know, she has not once spoken for those children. Later, I'll refer to a letter she wrote to us about the PIPEDA legislation and what the discretion really is for ISPs.

In the letter, she says that ISPs may look at this on a case-by-case basis—frankly, a case-by-case basis is not good enough for us anyway—but nowhere did she talk about what her office is doing to raise the interests of those children. No one is speaking for them, and that's one of the reasons why we came here today. We're here to try to lend a voice to their concerns and their issues. What's being been done to protect their privacy rights? We have to balance that with the privacy rights of Internet users, but part of the equation has to be the privacy interests of those children.

The issue for us has been raised in the media by law enforcement and in a couple of court cases. It's with respect to subsection 7(3) of the legislation, which sets out the provisions where an organization may disclose personal information. The first condition, as you will see, is with a warrant. Obviously, if police go get a warrant, then the ISP has to comply.

There is, unfortunately, some confusion with the second stipulation, which refers to a response to a request by a government institution that has lawful authority to obtain the personal information for the purpose of enforcing a law, carrying out an investigation, or gathering intelligence. It's that issue of "lawful authority" I think that has led to some confusion, and our basic suggestion to you is to clarify that.

There was a case in Ontario in which Toronto police were investigating someone. They sent a letter of request for information, pursuant to a child exploitation investigation, to Bell Canada. Bell Canada cooperated with that and provided information to the police, but this was challenged in court. At that time, the court said that the section I referred to does not establish what "lawful authority" is. The court went on to say that really, in that court's mind, a warrant was needed. Fortunately, that decision was overturned by a higher court. And just for your information, the search led to the discovery of a large child pornography collection.

But that's the issue that this committee should task itself with. What is lawful authority? If law enforcement were here to speak to this—and I would encourage you to actually have some of the investigators come to talk about their experiences with PIPEDA—I think what you will find is that a lot of the larger ISPs tend to cooperate with law enforcement even if they don't get warrants but just have letters of authorization. Not all of them do, though. For some ISPs, use of PIPEDA is left to their interpretation. We're asking for your committee to clarify that or recommend that it be clarified.

People ask why police don't just get warrants. One of your previous witnesses, I think from the industry department, referred to the speed with which these things sometimes happen. At the time, I think the chair actually asked a question about a case from St. Thomas, where there was live abuse going on with a child. Sometimes there just isn't time to go get a warrant.

The other thing, from our perspective, is that police don't need a warrant. What we're talking about is someone's name and address, which they can get off a licence plate. They don't need a warrant to get your name and address if they see you speeding away from the scene of a crime or failing to stop. Are we really going to give better protection or more enforcement for people who fail to stop than we are for those who might be abusing children?

In some jurisdictions, some pawn shops are required to have information about customers who come in and sell merchandise. That information can be used to track back stolen property. Is stolen property really more important than our children?

That's the basic thrust of our testimony here today. Again, we're not experts in law enforcement, but these are the concerns that law enforcement have expressed both publicly and to us, if you look at some of the media reports. Just last week, over this bust, you'll note that the head of the National Child Exploitation Coordination Centre, from the RCMP here in Ottawa, said we have to rely on ISPs to help us. Frankly, we don't think there should be any discretion for ISPs to help law enforcement, certainly in these cases. At the minimum, though, we would ask this committee to clarify subsection 7(3).

We would also ask that some consideration be given to perhaps amending the statement of principles of the legislation, to make it clear that the legislation was never intended to negate or interfere with the moral and ethical duties of companies. Companies will often complain about the costs of these things, about what it costs them to cooperate with law enforcement. It's our argument that we all have a duty to cooperate with law enforcement. We're seeing now, in British Columbia, twelve citizens potentially giving a year of their life to jury duty. We all have to do that. There are consequences and there are costs for us to do that.

● (0910)

We work with women who are abused by partners, who testify in court and put themselves sometimes at great risk to assist with the enforcement of the law. We're all part of the solution here, and I think it's incumbent upon ISPs to step up and do their part.

I can speak a little more to the cost issue if that's something you want me to speak to.

The last issue I would raise is whether this committee could use its influence to encourage the Privacy Commissioner to take a more active role in protecting the privacy interests of children.

Thank you, Mr. Chair.

The Chair: Thank you, Mr. Sullivan.

We will now go to the Insurance Brokers Association.

Mr. Masnyk, go ahead, sir.

[*Translation*]

Mr. Steve Masnyk (Manager of Communications, Insurance Brokers Association of Canada): Thank you, Mr. Chairman.

Good morning everyone. My name is Steve Masnyk. I am the Manager of Communications for the Insurance Brokers Association of Canada. Through its 11 provincial and regional members, the Insurance Brokers Association of Canada represents over 30,000 insurance brokers who are living and working in almost every community of our country.

Mr. Bob Kimball and Mr. Peter Fredericks, who are respectively the Chairman and the Vice-Chairman of our association, are with me this morning. I would like to leave the floor to Mr. Kimball who will be followed by Mr. Fredericks.

[*English*]

Mr. Robert Kimball (Chairman, Insurance Brokers Association of Canada): Good morning, everyone. As Mr. Masnyk mentioned, my name is Bob Kimball and I'm the volunteer chair for the Insurance Brokers Association of Canada.

I come from a small town of about 4,500 people, Sussex, New Brunswick. I just want to give you a little perspective on where I come from. I have six employees in my office. That includes me and my wife. My father is an insurance broker. My three brothers are insurance brokers. I mentioned my wife is an insurance broker. Even my son is working in insurance, so it's a family business...small community. Insurance gets in your blood.

My goal this morning is to provide you with an industry perspective as well as a working perspective on these issues that you're challenged to look into.

First, I'd like to commend your dedication in serving the public on an important issue that affects Canadians.

Privacy is one of the cornerstones of our society and something that should never wilfully be compromised. We live in a world that is being transformed by the greatest evolution in technology in our history, and safeguards need to be in place to protect Canadians from any abuses of their privacy.

I'm here as an insurance broker, so I'll speak on how some of the issues before you affect our profession and our consumers of insurance.

I'd like to begin this morning with a comment on the general effectiveness of PIPEDA. Through our experience, I would suggest to the committee that PIPEDA works, and it works well. I can tell you that we've checked with our office, the Insurance Brokers Association of Canada, and we have not received a single complaint regarding privacy since PIPEDA came into effect. In addition, we have confirmed with the general insurance ombudsman that his office has not received a single complaint regarding breaches of privacy when it comes to brokerages. It's based on this that I'm of the opinion that the approach taken in the spirit and the intention of PIPEDA has been a correct one.

After the privacy legislation was passed in 2001, our association prepared and distributed a guide to all of our brokers dealing with the implementation of these provisions, and you all have a copy of it in the binder.

In addition, we had seminars and road shows that were offered to all of our brokerages across the country to help them implement the new requirements. Brokers have embraced the guidelines as a regular part of day-to-day business. As brokers, we strive to cover and protect our clients. This is what we do every day. We provide clients with peace of mind. We would not be in business if we did not do this well.

Under this protective coverage also comes our clients' personal information. I'd like to share with you what that means in an insurance broker's office. In my own office, as well as having all of the physical things looked after—bars on windows, alarm systems, metal filing cabinets, those types of things—we have long-term employees. My shortest-term employee has been with me for 10 years. I have one lady who's been with us for 43 years. So we have long-term employees. We're in a small town, so obviously we have to keep people's privacy utmost in our mind.

Our computer system, which has the information in it, is a proprietary system. It doesn't work on a Windows base. It's very different. There are about six or seven different insurance systems out there, and you have to know entirely how the system works in order to get any information out of it. There are multiple passwords. We have passwords to sign our computers on, to get into our insurance system, to access information. So we take privacy very much to heart.

I'd like to ask Mr. Fredericks to address some of the issues that are raised in your consultation, if I could, at this time.

● (0915)

Mr. Peter Fredericks (Vice-President, Insurance Brokers Association of Canada): Thanks, Bob.

Good morning, everyone. My name is Peter Fredericks. I'm the vice-president of our association. As is Mr. Kimball, I'm a working broker in Bedford, Nova Scotia, a town of about 28,000. There are five other brokers in my town, actually. I employ four people.

Our day-to-day operation, from a security and privacy standpoint, is very similar to Mr. Kimball's, so I won't go through that again with you.

We have three issues we would like to raise on the Privacy Commissioner this morning. The first is the actual role and mandate of the Office of the Privacy Commissioner. We believe the ombudsman model is the appropriate and effective model for this organization. We believe it is essential that parties have access to collaborative dispute resolution, and we believe it is a fair practice to have a judicious overseer.

The second issue we wish to bring up is work product. It's an area that we believe needs clarification. It's widely accepted that information obtained during the usual course of business is proprietary to the firm. The current law, we feel, is unclear both in the definition of work product and in the fact that it should be excluded from falling under personal information. Our position is that the analysis and expertise surrounding the use of personal information is proprietary to the broker and should not be included in personal information under the law.

Our third issue is with respect to duty to notify in the event of a breach of personal information. We concede and agree wholeheartedly that this is a sensitive topic for all Canadians. Our profession is one that is based on assessing risk and placing it with the proper coverages.

Our basic reason for being is to protect our clients, whether it's protecting their homes, their cars, their business, or of course their privacy. It just flows that a breach in privacy would necessarily involve assessing the degree of breach, informing a client, and mitigating any future breaches—it's key to our profession. We believe it just makes good business sense to follow this model. Because of the nature of the insurance industry, we believe that regulating this duty would be challenging at best and practically unworkable at worst.

For us, the bottom line is that if a briefcase containing three clients' files is stolen, obviously the broker involved is going to make every effort possible to assist those three customers and do whatever is right to make sure that information is protected. Our concern is being regulated by this body to contact, in my case, all 2,500 of my customers to inform them that three customers' files had been stolen.

Those are basically our concerns with the issues before you. We'd like to thank you very much for the opportunity to be here this morning. We're more than happy to answer any questions you may have.

● (0920)

The Chair: Thank you very much.

Now we'll turn to Mr. Pecknold from the Canadian Association of Chiefs of Police.

Mr. Clayton Pecknold (Co-Chair, Law Amendments Committee, Canadian Association of Chiefs of Police): Good morning, Mr. Chair, and thank you.

I have some prepared remarks I would like to put on the record, if you will permit me. There will be some overlap I think with my friends from the Canadian Resource Centre for Victims of Crime, but if you bear with me, I'll go through them.

As stated, my name is Clayton Pecknold. I'm a deputy chief constable with the Central Saanich Police Service in British Columbia. I'm the co-chair of the Law Amendments Committee of the Canadian Association of Chiefs of Police.

First let me thank you for granting the CACP the opportunity on such short notice to appear before you today. I understand you are coming to the latter stages of your work and no doubt have had much material placed before you. I will endeavour to keep my remarks focused and brief with that in mind. I also wish to convey to you, Mr. Chair and members of the committee, the compliments of our president, Mr. Jack Ewatski, who's the chief of the Winnipeg Police Service, and our executive director, Mr. Peter Cuthbert.

The Canadian Association of Chiefs of Police represents the leadership of policing in Canada. Our membership spans all levels of policing, from municipal to federal agencies, and includes approximately 90% of the chiefs, deputy chiefs, and other senior executives from our nation's policing community. The CACP is committed to promoting effective law enforcement in Canada to the benefit and safety and security of all Canadians. As part of this mandate, and to enhance the effectiveness of policing, the CACP is committed to legislative reform such as that which is before you today. We appear often on bills and participate with enthusiasm and at every opportunity to consult with government on matters pertaining to the law and policy having an impact on public safety.

As I have stated, I'll endeavour to limit my remarks and therefore will focus primarily on two sections of the act. Before moving to specifics, permit me some general comments both to provide illumination of the guiding principles under which the CACP carries out its mandate, but further to provide some comment about the general policing environment in Canada, so that this honourable committee may have some context in which to view our specific comments.

The overall goal of the CACP is to lead progressive change in policing through, among other things, the advocacy for legislative reform, the advancing of innovative solutions to crime and public order issues, and the promotion of the highest professional and ethical standards for its member agencies. Simply put, the CACP believes that preserving and respecting the rule of law and the Charter of Rights and Freedoms guarantees that we will maintain the continuing consent of the citizens we police.

With the foregoing in mind, allow me to state clearly that the Canadian police community is very mindful of the concerns of Canadians for their privacy. We, like all Canadians, understand that while the digital age has brought forth much benefit, the ease with which personal information flows across boundaries brings with it many challenges for law enforcement. My committee and other CACP committees, such as the electronic crime committee and the organized crime committee, are actively pursuing legislative and policy initiatives to combat privacy-related criminal activity such as identity theft and telemarketing fraud, to name but two.

As well, as police services have modernized our own electronic data collection and information-sharing practices, we have worked hard to place the appropriate safeguards in place to ensure we comply with both the spirit and intent of our various governing privacy acts and the fair information practices they enshrine. We are also mindful that Canadians have a growing awareness of the very real dangers posed to our society by organized crime, global terrorism, and, perhaps most alarming, the exploitation of our children by Internet predators and purveyors of child pornography.

To that end, the CACP continues to advocate for changes to our laws to provide a balanced and effective set of investigative tools to deal with the new challenges faced by law enforcement in the information age. While Canadians expect balance and restraint from their police, they also expect that we will have the tools available to us to keep them safe and serve the public interest.

Another point I would make is that policing is not strictly the enforcing of laws. While the investigation of crime and the apprehension of criminals is a key aspect of what we do, provincial police statutes in the common law recognize that the primary duty of a police officer is the protection of the public and the preservation of the peace. In pursuit of this we are often called upon to perform tasks that are of a social benefit. These include such tasks as notification of the next of kin, checks on the welfare of the elderly and infirm, assistance to child protection authorities, or working in collaboration with mental health professionals to assist in protecting vulnerable persons within our society. In any or all of these cases, police may need timely access to accurate information about an individual for the benefit of that individual or for some other public good.

● (0925)

Therefore, here are some key points I would ask that you draw from my opening comments.

First, the digital age and the new realities of the Internet and the free flow of personal information in electronic form pose many of the same challenges to effective policing as they do for other sectors of society and, we suggest, have brought with them new public safety challenges.

Second, police operate under the considerable scrutiny of the public, the courts, and other regulatory bodies. Every police agency in this country is governed by privacy legislation. We understand our responsibilities with respect to the protection of the privacy of Canadians.

Finally, while one may tend to think of policing in terms of enforcement of the criminal law, there are many everyday functions performed by the police that do not invoke the criminal law powers or the associated investigative authorities, yet are equally of service to the public good.

Now turning to the act specifically, I would like to comment on two areas: the disclosure by police of personal information without consent, and secondly, the disclosure of information police themselves request to the individual about whom the information was requested. Specifically, I'm talking of sections 7 and 9.

As you know, paragraph 7(3)(c) permits organizations to disclose personal information without the knowledge or consent of the individual, where a court order exists. Police do frequently seek information with prior judicial authorization under search warrant or production order when the information is of a nature that attracts section 8 of the charter protection and of course where they can meet the legal threshold for obtaining such an order. But as noted, there are occasions in which information sought does not attract section 8 protection. One example of this is hydro power usage, which may indicate the theft of electricity or operation of a marijuana grow-op. There is some good authority from the courts that a warrant is not required for this information.

In another example, a police officer may be in the early stages of a missing person investigation, in which he or she is trying to determine if in fact a crime has occurred. Perhaps we may have to solicit the assistance of a financial institution because we need to know if that person bought gas at a particular gas station or if the person used a credit card, or perhaps we need to find out if a person has a cell phone registered to him with a particular company. For this information we rely on paragraph 7(3)(c.1), which permits disclosure upon lawful authority, as my friend has already noticed. However, we are increasingly seeing some companies interpreting lawful authority to mean that a warrant or court order is required before they comply. This is an interpretation that is not, in our respectful view, consistent with the intent of the drafting of the act. Such an interpretation by companies, while no doubt grounded in a legitimate desire to protect their customers' privacy, is overly restrictive and defeats, in our view, the intent of paragraph 7(3)(c.1). That section is intended to be permissive and give guidance to the holder of the information to ensure that there is some legal basis upon which the police are requesting the information. That legal basis may be a criminal investigation and may involve the service of a court order, in which case paragraph 7(3)(c) would apply, or it may be pursuant to our many other duties, in which case we suggest that paragraph 7 (3)(c.1) contemplates a situation in which a warrant is not required or indeed available. It does so by using the term “lawful authority” and differentiating between the enforcement of a law and the carrying out of an investigation relating to the enforcement of the law.

It is important to note at this juncture that the police are always restrained by the rules of evidence, and wherever there is an expectation that information is to be used for criminal prosecution, we are careful to ensure we do not jeopardize the subsequent prosecution by obtaining evidence in a manner that would otherwise require a warrant.

The second section concerned is section 9, which provides that a person may have access to his information possessed by the company, including whether the company has disclosed that information to another party, including the police. There is, of course, a provision that permits the objection by law enforcement to disclosure of the fact that a request had been made for the information, but as we understand it, the prevailing view of that section and the cumulative effect of that section are that protection is triggered only when the individual actually makes a request. In our view, there is nothing preventing a company from adopting a policy of voluntary notice to customers that the police had requested and received information. This is, as you can no doubt appreciate, of concern for us, most especially when there's an ongoing and sensitive investigation or the information was requested for intelligence purposes.

For purposes of the end result, we are requesting that the committee consider clarifying the ambiguity in sections 7 and 9. First, we respectfully suggest you consider clarifying the term “lawful authority”, either within the definitions section of the act or by employing some other wording, which would clearly demonstrate that a warrant is not required. This is recognizing, of course, that section 7 is permissive and that companies are not compelled to provide the information. Such clarification would serve primarily to give them some comfort in their efforts to be good corporate citizens and, where appropriate, assist in matters of public safety.

With respect to section 9, one possible suggestion is that an amendment be made to generally prohibit the disclosure to an individual that the police have requested or received information, regardless of whether the request is made by the individual. Provision could be made for the police to consent and not unreasonably withhold that consent. Such an amendment would also help clarify the obligations of companies, of course.

● (0930)

In closing, it is important to notice that the vast majority of organizations covered by the act strive to be good corporate citizens. Police across this country work closely with all members of their respective communities, corporate or otherwise, to maintain professional and cooperative relationships. This is a key component of good police work.

In keeping with this, it is important that all parties have a clear understanding of their duties and obligations with respect to protecting Canadians' privacy. Clarity of language in the act will go far in ensuring the appropriate balance between the protection of that privacy and the needs of public safety, by making sure the right information goes to the right people at the right time and according to the law.

Once again, on behalf of the Canadian Association of Chiefs of Police, thank you for the opportunity to comment.

The Chair: Thank you very much.

Just before we go to questions, Mr. Sullivan and Mr. Pecknold, I know neither of you are lawyers, but do either of you have any knowledge of whether the phrase “lawful authority” has been judicially interpreted by any court of appeal or the Supreme Court of Canada?

Mr. Steve Sullivan: It hasn't, to my knowledge.

Mr. Clayton Pecknold: I am a lawyer and I don't think it has. I did a quick search and didn't see it.

The Chair: All right. Thank you.

Mr. Dhaliwal.

Mr. Sukh Dhaliwal (Newton—North Delta, Lib.): Thank you, Mr. Chair.

First of all, I'd like to thank everyone who has come here today.

Mr. Sullivan, you said that ISPs should have the discretion, at a minimum, to be utilized to work with the police on the issues. I commend you for coming out and speaking for the children.

Are there any ISPs that are not cooperating with the police agencies at this time, and what would be the circumstances?

Mr. Steve Sullivan: It's my understanding that most of the bigger ISPs generally cooperate with law enforcement. According to the Privacy Commissioner, in a letter we received from her, ISPs look at it on a case-by-case basis, so I guess it depends on the circumstances and what the issues are.

I'll refer to the *Edmonton Journal* of February 8. The head of the RCMP's coordination centre referred to some smaller Internet service providers that exist solely to trade in child sexual abuse, and the challenges in getting smaller companies to cooperate. Our concern is that if we leave it voluntary, the bigger companies will cooperate, but the people who are trading this stuff know what's going on and they'll tend to go to the smaller companies that are not cooperating.

I will refer very briefly to legislation that the former government introduced, Bill C-74, prior to the last election. It would have spoken to the issue of requiring ISPs to cooperate with law enforcement.

● (0935)

Mr. Sukh Dhaliwal: You said you have some costs associated with it. Do you have those numbers?

Mr. Steve Sullivan: What I was referring to there is in our brief, and again I apologize for not getting it in sooner. There was a case in Toronto where the police were looking to get information. I think it was a homicide investigation. The issue the ISP raised was that the cost of cooperating with law enforcement would be an unreasonable financial burden. It's the only example I know of where the costs were actually discussed.

The court heard evidence on the complete annual cost for companies to comply with production orders—orders from the police to get information. The complete annual cost was $660,000. The court had a forensic auditor look at those numbers, and they found that the expenditure was 0.0087% of Telus' operating revenue and 0.012% of their net income for one year. So the forensic auditor said it was not really a material amount. When you look at the profit compared to the cost of cooperating with law enforcement, we're really talking about fairly minimal numbers.

Mr. Sukh Dhaliwal: Do you see a role that these Internet service providers can play beyond just sharing information with the police when it comes to the exploitation of children?

Mr. Steve Sullivan: Ideally we would like to see ISPs take a more active role in ensuring that their services are not being used to facilitate the exploitation of children. That doesn't mean they have to police the Internet; that's unreasonable. But certainly when they become aware of how their services are being used, they should be more proactive in cooperating with law enforcement.

Certainly at a minimum, when police come and ask for help, they have an obligation to assist. But if there are ways for them to be more proactive in trying to reduce the chances that their own services, what they're making money from, are being used to exploit children, that's an issue to be explored.

Mr. Sukh Dhaliwal: Mr. Pecknold, do you have any comments to add?

Mr. Clayton Pecknold: There's a bit of a crossover on this issue, especially with respect to cost during the ongoing lawful access consultations we've had over the last number of years, which my friend alluded to, the Modernization of Investigative Techniques Act, the bill that was introduced by the previous government.

The Telus Mobility case is going before the Supreme Court of Canada, actually. That's the case that dealt with the imposition of a fee by Telus at the time as a precondition for complying with an order for production of data. The Supreme Court, it is my understanding, has granted leave to appeal. The CACP is considering intervening in that case.

What we found is that the deregulation of the telecommunications industry has produced a lot of small players in the industry. We have consulted with them, and we're mindful of the challenges they have in complying with requests from law enforcement. A lot of these ISPs are mom and pop operations, and they operate on a very thin margin, profit-wise. They tend to be good corporate citizens, and we know that. They want to comply, but there's an impact to complying.

We do find also, though, that there's perhaps some concern with respect to their liability if they produce information without a warrant, when in fact a warrant isn't required or we don't have a warrant available. We try to give them some comfort and clarity as to what's required.

By and large, we do run into some challenges, that's true. There are probably no doubt examples of blatant disregard, but I would say those are the exceptions, not the rule. That's why we look for clarity in terms of the tools, and we look for the tools necessary to get the information to us. The other concern, obviously, is that ISPs' data is erased quickly, so we need to get to it quickly. That's an area of concern for us that the MITA legislation was intended to address as well.

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

The Chair: Thank you.

[*Translation*]

Mr. Vincent, you have seven minutes.

Mr. Robert Vincent (Shefford, BQ): I am very happy that you came here today and presented us with this information.

Mr. Sullivan, if I understand you correctly, you would like that ISPs be allowed to disclose information when an Internet site contains child pornography. Is that correct?

[*English*]

Mr. Steve Sullivan: I'm saying they have the discretion to cooperate with law enforcement. When law enforcement makes a request to get the name of a potential suspect—subscriber information, name and address—they have a discretion to cooperate with law enforcement.

I think according to the legislation there's been some confusion, and Mr. Pecknold has referred to that, as to whether the companies can or can't without a warrant.

● (0940)

[*Translation*]

Mr. Robert Vincent: What are you recommending? Do you recommend that ISPs be allowed to disclose that kind of information to th police? The same principle might apply to any other service, such as insurance, or any type of situation, for instance in case of theft. I understand that you would like the possibility to share information with law enforcement in any kind of investigation. Is that right?

[*English*]

Mr. Steve Sullivan: Obviously, our interest is Internet service providers because that's an area where children are being exploited by the Internet. Our recommendation is—and I only speak to the area of the Internet because that's the issue we're dealing with, children being exploited—that the legislation should be clarified so that the companies can provide information when police have lawful authority and make that request, and I think it should define what lawful authority means.

Also, we would go beyond that and say that certainly in the cases of child sexual exploitation, Internet service companies should not even have a discretion; that when police come and make a case that they need information, they should be required to share that information. That would be consistent with the legislation the former government introduced, Bill C-74, that would have made those requirements that companies had to cooperate with law enforcement.

[*Translation*]

Mr. Robert Vincent: But you do not entirely agree with Mr. Pecknold who said that gas stations, stores, and so on, should provide that information when there is an investigation. You are only referring to the Internet and you do not want to authorize the police to investigate and obtain personal information on anyone at any time.

[*English*]

Mr. Steve Sullivan: I'm not saying there aren't other areas. I'm only speaking from our experience, so our comments are limited to the Internet service providers.

[*Translation*]

Mr. Robert Vincent: Mr. Pecknold, I shall ask you the same question. Why should all kinds of personal information be shared with law enforcement when there is an investigation? Don't you fear that some police officers might abuse their power and pretend that they are conducting an investigation just to get information about someone?

[*English*]

Mr. Clayton Pecknold: First of all, let me clarify what type of information we're talking about. For example, when we're talking about ISPs, we're talking about customer name and address information. We're not talking about their Internet usage, we're not talking about what websites they've searched, or that sort of private information that would attract the necessity for us to obtain a warrant.

What we're talking about is saying to an ISP, or to a company or a gas station or a financial institution, that we're looking for so-and-so, and we're wondering if so-and-so is one of their customers, yes or no. That then allows us to go on a line of inquiry that may ultimately allow us to obtain the proper authorization to get the information for which we would require a warrant. What we find, though, is that some interpretations of the act are limiting some companies from actually telling us whether or not there is a customer there. We obviously then have a number of investigative steps we have to take when they don't allow us to get that information.

So for what we're looking for, we're talking about information that does not attract the section 8 charter protection. We're certainly not looking to read people's e-mails without warrant or go into their Internet usage without warrant. We would never ask for that. We don't intend to ask for that, and it's not the direction we're going in.

[*Translation*]

Mr. Robert Vincent: Mr. Kimball, you said earlier that if you did lose three files, you would call those 2,500 clients. Do you consider it important? The representatives of other insurance companies told us that in that kind of situation, the decision to inform or not inform their clients was left to their discretion.

You work with a limited number of employees, but you make it your duty to call all your clients as soon as a file or information is lost in order to verify with them if that file contained personal information, don't you?

● (0945)

[*English*]

Mr. Robert Kimball: Thank you.

Luckily, first, we've never had any incident whatsoever of having a lost file. We do believe that if there is a file lost, we have to protect our client. That's the business we're in. We should notify that client and make sure we learn from whatever happened to make us lose that file.

Our question is whether or not it would be appropriate to worry all of the clients we have if, for instance, one file happened to be stolen from a briefcase while I was out visiting a client. We would not want to worry all of the clients when there was no possibility of a breach to them.

The business we're in as brokers is the protection business, so if some people are breached, we definitely want to let those people know so that they can protect themselves. We don't really feel it would be appropriate to worry all of the people who would be unaffected. We don't feel there would be any real benefit there.

I hope that answers your question.

[*Translation*]

Mr. Robert Vincent: On what basis do you decide to tell or not tell your clients that personal information has been stolen from your files? How do you evaluate the risk?

[*English*]

Mr. Robert Kimball: Again, luckily, I have no experience at this, and virtually most brokers have not. What we have is the regular protection in our office, to make sure there hasn't been a breach, with the alarms, locks, etc. If there were a breach, we would look to what information we have, talk to that client, and let them know.

As insurance brokers, we do not carry or do not have very much information in our offices. For instance, we do not even collect social insurance numbers from our clients. We have no use for that information; therefore, we do not collect that. The amount of information we have is very limited.

We would let clients know right away if there was a breach, that their file went missing—here's the information we would have—and we would work with them to try to lessen whatever damage might affect them.

The Chair: Thank you, Mr. Vincent.

Just before we go to Mr. Wallace, who is next, Mr. Sullivan and Mr. Pecknold, I understand you have a concern with the alleged vagueness of the term “lawful authority” in subsection 7(3). Are you concerned at all about the word “may” in the operative portion of the subsection? The reason I ask is that the way it reads, “an organization may disclose” only if, for example, required to comply with a subpoena. Are you concerned that somebody might say that “may” is permissive and not requiring? I'm just wondering.

Particularly in deference to the judiciary, as I found out in another committee I'm on, “may” is a very common drafting term. I don't know if you've highlighted any concerns. Maybe they're just my concerns. I'm just asking if you have concerns with the word “may”, and let's use it specifically as linked to paragraph 7(3)(c), because it would seem to me that if there's a subpoena or warrant, it should be “shall”. There should be no discretion if it's in accordance with a subpoena or warrant.

So that's just a quick question. Do you have concerns with the use of the word “may” in subsection 7(3)?

Mr. Clayton Pecknold: I hadn't noticed that, Mr. Chair, but what you're noticing there is in fact the problem in the Telus Mobility case. If you look at that word “may”, it conflicts with the fact that, in our view, a court order is a must. That always seems self-evident to us, but what we're finding is that, especially when electronic data is archived or there is some cost to the company to produce the data or get it out of archives, they view their ability to set a fee as a precondition for compliance with that court order. The CACP is on record as saying very clearly that this is an erosion of the authority of the courts, and that if the legislation doesn't provide for a fee, there is no fee. An order of the court is an order of the court is an order of the court.

The Chair: To my way of thinking, what the drafters really meant instead of “may” was “is permitted to”, because this is a description of when organizations are permitted to release information without consent. Rather than the word “may”, I think what was meant was “is permitted to disclose personal information”, etc., whereas “may” could give the impression that there's some discretion.

Thank you.

Mr. Wallace.

● (0950)

Mr. Mike Wallace (Burlington, CPC): Thank you, Mr. Chairman. I will ask all three groups a question or two, but I'm going to start with the insurance group.

You talked about work product, and it's unclear in this legislation nationally. I think there are definitions in the privacy legislation provincially in Alberta and British Columbia, and possibly in Quebec, although I'm not positive about Quebec's.

My first question is whether or not you have a definition with you. Do you have any changes to the wording that you would like to see in the legislation at present?

Mr. Peter Fredericks: No, and I apologize for that. We haven't actually gotten that far with it. What we look at is proprietary. As an example, if I insure your home, I have to get information from you. You may provide me with photos of your home, you may provide me with a photo of your wood stove, or you may provide me with different appraisals on jewellery items. Those would certainly be considered to be your personal items, and in the event that we no longer did business, you would certainly be entitled to get those things back. We have no concern with that.

What we're looking at is when we do, for example, a calculator. You provide me with the information on your home, the number of floors, the square footage, the number of bathrooms, and the built-in kitchen appliances. From that, I would use a calculator that would determine the value of your home. It's a product that each insurance broker would buy from three different providers.

In the event that you chose to take your business elsewhere, we would feel that particular piece would in fact belong to the brokerage. It would really give you an advantage or give your next broker or direct writer an advantage if we had to provide that to you.

Mr. Mike Wallace: Just so I am absolutely clear, you're obviously not opposed to notification. Right now the legislation nationally is working with the commissioner on whether notification is required or not, but there is some discussion about making notification a requirement. You'd like it to be narrow enough or specific enough to apply to those who are directly affected, and not to everybody who is generally a customer, for example. Is that correct?

Mr. Peter Fredericks: That is absolutely the case.

Mr. Mike Wallace: My next question is for the police association.

Again, section 7 talks about lawful authority, which you were just talking about. Do you have a new definition for us at all? Have you worked on that? I've been asking every delegation we've seen since the beginning of time on this review whether they had specific wording or not. Do you have specific wording on that particular issue?

Mr. Clayton Pecknold: No, I haven't put my mind to it, and it would probably be dangerous for me to try to draft legislation on the fly, but the key point for us, obviously, is the clarity that it's those circumstances that don't require a warrant.

Mr. Mike Wallace: Okay.

Then in section 9, about prohibition of disclosure to police, you'd like to see the wording changed, if I heard you correctly, so they don't have a choice, in a sense. They disclose to you, the police, and then you have the option of consenting that it be disclosed to those whom you may be investigating. Is that an accurate statement?

Mr. Clayton Pecknold: Well, obviously, our ability to withhold consent would have to be reviewable by the Privacy Commissioner. We'd make the point that it can't be absolute. We understand there has to be a mechanism of oversight. But rather than it being triggered by a request and then a subsequent objection, we would just like to see it mandatory that they not disclose the fact that we requested the information, unless the Privacy Commissioner so orders, for example.

Mr. Mike Wallace: Okay. Do you know if that exists in the other privacy legislation, in provincial privacy legislation?

If you don't know, it's fine. We'll find out.

Mr. Clayton Pecknold: Well, it takes me back to when I practised privacy law.

I don't know, actually. I should not say.

Mr. Mike Wallace: Okay. So we need to find that out, if we could, whether that exists.

Now to my friends from the Canadian Resource Centre for Victims of Crime, you're here today mostly in regard to Internet service providers. Again, you're interested in a better definition of “lawful authority”. Would that be correct? Let me get this clear.

Mr. Steve Sullivan: Yes.

Mr. Mike Wallace: One thing that no one else has really mentioned about the preamble or statement or principles, or whatever we call it at the beginning of the bill, is.... Would you actually like to see something added to that to do with working with the police? I'm not exactly sure what you are looking for there.

● (0955)

Mr. Steve Sullivan: I think what we'd like to see is some clarification that PIPEDA was never intended to negate or interfere with people's moral and lawful duties to be good corporate citizens in assisting the police. Obviously our issue comes back to protecting children, but if there's a way to incorporate the notion that children have a right to privacy, that is certainly a paramount consideration in cases of child sexual exploitation.

Mr. Mike Wallace: Since you are here and this is a privacy issue, I have a private member's bill, Bill C-279, that deals with the DNA of missing persons. I hope it is going to committee next month. What it really does is to allow a loved one to bring in a hair sample, or whatever the DNA match might be, and allow them to attempt to find people who have been missing. There are issues about timing, and let's use the argument that it's been over a year. There are over 6,000 people missing, and a year seems to be the magic number, as 80% of missing people are found before the year is up. But there are a number who are not, and it's very difficult, even if the missing person has deceased, to go from morgue to morgue to find whether your relative is there.

There is one small issue about privacy, which is that the person you're looking for has not consented to their DNA being reviewed. Before I go before committee, I would like to know if the resource centre has looked at this at all and has any issue with the legislation.

Mr. Steve Sullivan: In fact, we've had a long-term interest in the issue and in the bill. We have been working in particular with one a lady from British Columbia whose daughter has been missing for a number of years. She's been very vocal on this issue. We've worked with your predecessor, Mr. Lunn, who introduced a similar bill in the previous Parliament.

We did a study for the Department of Justice on families with unsolved homicides, and in some of those cases there were loved ones who were never found, although foul play was suspected, and the toll is just tremendous, especially on parents.

I know there were privacy concerns raised. My understanding is that the DNA missing person's index, or whatever the appropriate term is, was going to be included in the first round of the DNA data bank back in 2000, but there were some concerns raised by women's groups about the privacy of potential clients who might be fleeing abusive relationships. I think those are fair concerns. I think we can probably address both. What we're really talking about from our perspective is the parents of missing children who come in and give their DNA—or the DNA of their child, if they have a brush or some hair or something—which can be compared with an index or database of unidentified human remains in coroners' offices.

So I think there's a way to balance those privacy interests, so that if police were to find someone alive and well and living in B.C. and who doesn't want their loved ones...then maybe there's a way to speak to them first before letting people know. I think there are ways to deal with those issues, but given the comfort that some families might get from knowing what happened, it is definitely worth proceeding with.

Mr. Mike Wallace: Thank you very much.

The Chair: Just for the committee's information, our researcher—always on top of the issues—points out that section 20 of the Alberta act says that an organization may disclose, etc., but only if "(f) the disclosure of the information is to a public body or a law enforcement agency in Canada to assist in an investigation". So that's something we should take into consideration, since the Alberta act was brought in after PIPEDA.

We'll go to Mr. Peterson, followed by Mr. Reid. This is a five-minute round.

Hon. Jim Peterson (Willowdale, Lib.): Again, the Alberta act uses the word "may".

The Chair: Yes, I noticed.

Hon. Jim Peterson: You would like something more compelling, such as "must"?

Mr. Steve Sullivan: From our point of view, certainly with reference to where it says there should be a warrant, obviously we agree with our friend that if there's a warrant, that's a must. There should be no discretion.

Hon. Jim Peterson: We understand that, but where there isn't a warrant.... You made the point very aptly that in many cases you don't have time to do these sorts of things. It would be very helpful to us if you could put your heads together to come up with the exact wording you would like to see.

● (1000)

Mr. Steve Sullivan: I don't want to speak for my friend, but from our perspective, in cases of child exploitation through the Internet, it should be "must". There should be no discretion for ISPs. I don't want to speak for anyone else, but that's our position.

Hon. Jim Peterson: Good. Okay.

Can you give us examples of how the police have been hindered in their investigations when people have not been forthcoming?

Mr. Steve Sullivan: I can only give you anecdotal examples that we've been told about by law enforcement. We've referred to some media articles as well in our brief. The *Edmonton Journal* article I referred to from last week even says that the head of the RCMP centre says, "We can't start without knowing a name and address.... The investigation is over if we can't get that information...". She says that most of the larger companies do cooperate, but some of the smaller ones don't.

I can't give you names and—

Hon. Jim Peterson: I just wanted to know how much of a problem it is.

You mentioned, Mr. Sullivan, that you want the Privacy Commissioner to play an enhanced role in tracking down child abusers. Could you be more specific as to what you would like to see the commissioner do?

Mr. Steve Sullivan: I wouldn't say that she would have a more enhanced role in tracking down abusers, but I'm thinking of a more enhanced role in looking into the issue of what ISPs could do, for example, to better assist law enforcement and to speak for the children and talk about their privacy interests as well as the privacy interests of customers.

One thing, for example, is that perhaps her office could do some research or investigation into what ISPs could do to remove the images when they are identified by law enforcement, to make sure they're taken off—those kinds of issues. I don't think the office has a law enforcement role, but she is an ombudsman advocate for privacy. I guess what we're asking is that her office be more proactive in speaking for the privacy rights of children in these cases, and to do research into the impact of....

We've included in our brief an impact statement from a young girl from the States who was abused over a number of years. Her adoptive father put her photos on the Internet. Her impact statement is used in the sentencing of offenders who are found to be in possession of her images. In it she says that one of the hardest parts is knowing that her images are still out there, still being used by men for their own sexual perversions.

We're saying that the Privacy Commissioner has a role to take in speaking for that child and other children out there.

Hon. Jim Peterson: I'm not sure how you retrieve all of those terrible images once they're out there.

Mr. Steve Sullivan: You're right; we won't. Say, for example, we identified a young girl from Ottawa, and we found that her father had identified images. I don't pretend to know the answer, but are there ways, are there things the ISPs could be doing to help law enforcement remove those photos? I think the Privacy Commissioner has a role in trying to answer those kinds of questions. I don't pretend to have those answers, but I think her office has the ability to try to shed some light.

You'll never remove all the photos. I don't pretend to be naive in that way.

Hon. Jim Peterson: Thank you.

The Chair: Thank you, Mr. Peterson.

Mr. Sullivan, you mentioned that you had a letter from the Privacy Commissioner. Will you table that with the committee if it isn't part of your submission?

Mr. Steve Sullivan: I did quote it. I'm certainly happy to provide a copy to the committee.

The Chair: Would you be sure to do that before we leave today?

Okay, we'll now have Mr. Reid, followed by Madame Bonsant.

Mr. Scott Reid (Lanark—Frontenac—Lennox and Addington, CPC): Thank you.

My question is also for Mr. Sullivan. It seems to me, when discussing child pornography, we're really dealing with two distinct offences. One is the original violation, which I guess could be generally characterized as a form of rape; and the second is the continued possession and circulation of the images after the fact. Of course, both are affronts to basic human dignity, but it seems to me they are different, in the same sense that robbery, which would be the homologue to the first of the offences, is distinct from possession of stolen property after the fact of the original offence.

In trying to think how to deal at a practical level with the second of the two offences, given that the first could have occurred at some point in the past, it might be impossible to identify the person to whom the violation occurred, and they may be deceased, for that matter. There is a very high probability that the original offence occurred outside of Canada—probably likelier than not, I suppose, as a statistical matter. I don't know that for sure, but it seems likely. Given that, if the second offence is treated as a form of possession of stolen property, it seems to me there is a logical pattern for dealing with it.

I noticed, actually, following this thought along, that you had made reference to the example of pawnshops and the requirements that are placed upon pawnshops. If we use the pawnshop as the analogy to an Internet service provider, I wonder if there is some direction there as to how the law ought to be recrafted in order to ensure some sort of more effective method of enforcing efforts to remove these images and their circulation.

● (1005)

Mr. Steve Sullivan: Yes. There are jurisdictions—certainly Ontario is one, and my friend can speak to others—where pawnshops are required to track the customers and the merchandise, and law enforcement can have access to that to try to trace back to who had the stolen property and maybe where it came from, and go from there. I think there is probably some guidance there.

I would say one thing about the difference between stolen property and child pornography, even if it is just possessing the photos. From our perspective, and I think from the victim's perspective, that is not just a form of possession; it is a form of abuse that someone is using those images of those children for that person's own satisfaction. We know that some offenders use it to break down the barriers of other children, to show them that maybe this is kind of normal and then facilitate their own abuse.

Mr. Scott Reid: That would seem to be a separate offence in addition to the basic possession, I would think.

Mr. Steve Sullivan: But I speak of that because to find out those people who possess that stuff may also prevent the abuse of other children. That heightens why it is especially important.

Mr. Scott Reid: Thank you.

Mrs. Krista Gray-Donald (Director of Research, Canadian Resource Centre for Victims of Crime): Perhaps I might speak to that.

There was an example in Gatineau this fall where police had identified someone who was distributing child pornography on the Internet, and when they were able to ascertain who it was, they did find that he was indeed abusing a child. So had they been denied the opportunity to have his information for just the possession of child pornography, they potentially would have missed the fact that this child was also being abused.

Mr. Scott Reid: Presumably, one can trace backwards. Assuming that the offence or the abuse is still ongoing, as opposed to something that occurred in the past, even if it's occurring outside of Canada, if we were able to get the information in an expeditious manner, that might actually help in tracing it backwards to other jurisdictions. Would that be correct?

Mr. Steve Sullivan: There is, and my friend can speak to this perhaps.

I know the Toronto Police Service has been very active in trying to track back through image analysis. You may remember the case of images they released, taking out the young girl's image but showing a hotel room or amusement park where she was being abused, and it actually led back to Disney and a hotel there. It turns out she'd had a rescue, but there is a lot of work being done by law enforcement, and some groundbreaking stuff here in Canada I think to track back.

One of the goals—and one of my friends spoke to it—is protecting the public, identifying these kids and rescuing them. It is not just about putting the bad guys away; it is about finding these kids who are being abused. So there is a lot of excellent work being done in that area.

The Chair: Thank you, Mr. Reid.

[*Translation*]

Welcome, Ms. Bonsant. You have five minutes.

Ms. France Bonsant (Compton—Stanstead, BQ): Thank you very much.

Mr. Sullivan, I am going to tell you about the child protection measures we have in the province of Quebec. I am not a lawyer, but these things are automatically protected on the Internet.

I understand that you are trying to eliminate Internet pornography. The problem does not exist solely in Canada but also at the international level. We should target all countries and tell them that they should start protecting their children. There is a lot of child pornography.

We are also hearing about soldier children who are wasting their life because they don't know anything else.

Your mandate is not limited to the Internet; it has an international scope. I wish you good luck, because we have many perverts in Canada who are going abroad to exploit children.

It is one thing to arrest those who are producing that kind of pornography on the Internet, but what do you do against the customers who download it and enjoy it? There are customers for that kind of pornography. If there is a demand, it is because there are customers. You should not only arrest the producers, but also the customers.

● (1010)

[*English*]

Mr. Steve Sullivan: That's absolutely the case. I agree with you on your first point about this being an international problem; we're certainly not naive about this being a Canadian problem. In cases like the one last week, when this huge child pornography ring was busted and our law enforcement was given the addresses—depending on what reports you read—of a number of Canadians, it's important that ISPs cooperate, but I do recognize that it's an international challenge. Some countries don't do very much against the abuse of children, if not actually promoting it.

I agree with you about doing more than just catching the bad guys. Certainly our interest is in law enforcement efforts to identify and rescue children. I raised the issue of the Privacy Commissioner and if there's a role for her office in doing some research into the responsibility or ways for ISPs, when we identify a particular child, to take the child's image off their site, or their network, at least. I agree there's so much more to be done than just what we're talking about here today. It's a huge problem. I don't want to pretend to be naive about the solutions; I think this is one part of it, but there's much more work to be done.

[*Translation*]

Ms. France Bonsant: I find it terrible that we have to pass laws to protect our children because they are gifts from Heaven. It is a simple message to transmit to everyone.

I was a member of the Commission on Maher Arar. I have some difficulty with personal information requests. I know that some police officers do an excellent job—I have a brother who is a policeman— but there are others that are not very competent. In the case of Maher Arar, as they could not find all the personal information they were looking for, they fabricated some. I am rather emotional about it. If we make it too easy to access personal information, there might be some exceptional cases of abuse.

Law enforcement and some other people have access to information on divorces. There was a case in Montreal where a police officer managed to find his wife and gunned her down. I must admit that this case is extreme. However, we should be very careful when we give access to personal information because victims are women most of the time. The government wants to scrap the long-gun registry, but in cases of domestic disturbance, it is very important to know if there is a rifle in the home.

We should be very careful when personal information is requested on some people. I would like to know your opinion on this.

[*English*]

Mr. Clayton Pecknold: Thank you.

I have a point of clarification on the translation. You referred to a commission. Are you talking about the Arar report?

[*Translation*]

Ms. France Bonsant: Yes.

[*English*]

Mr. Clayton Pecknold: I have a few comments. First of all, I don't suggest you intended to imply this, but I don't believe the commissioner found in that inquiry that any information was manufactured by the RCMP.

[*Translation*]

Ms. France Bonsant: You should read the book.

[*English*]

Mr. Clayton Pecknold: In any event, I will say that a number of mechanisms are in place for us to deal with breaches of our policies, breaches of our laws, and breaches of our internal ethics and standards. Yes, there are abuses on occasion, and we take them very seriously as police leaders and police managers. We have a number of mechanisms of oversight and a number of complaint routes. We will prosecute criminally; I myself have prosecuted officers for breaches of privacy. Your concern is valid, Madam, but we take that very seriously. However, there is also a legitimate need for us to investigate the law and obtain information according to law and in an appropriate manner.

The Chair: Merci, Madame.

I've been fairly lenient, but I want to remind committee members that we're reviewing PIPEDA, the specific legislation, and we're talking about specific suggestions with respect to specific legislation, as opposed to other issues like private member's bills and the Maher Arar commission. I'd ask us to focus on PIPEDA if we could.

I'm going to Mr. Stanton, followed by Mr. Pearson, followed by Mr. Van Kesteren.

Mr. Bruce Stanton (Simcoe North, CPC): Thank you, Mr. Chair, and thank you to our panel this morning. It's been very insightful for our study of PIPEDA.

My question actually, first, is to our representatives from the Insurance Brokers Association, and I'll direct it to Mr. Kimball. The third item you talked about in the three areas, around which you had some suggestions that you touched on briefly, was the issue around the duty to notify. And of course that issue was in the news quite regularly several weeks ago as it related to CIBC, Winners, and so on. In your comments you suggested that this would be something that would be problematic to regulate, but you didn't go much further in your comments. I wonder if you could just expand on what your thoughts are about this duty to notify.

This is a topic that has come up in the course of our testimony and there have been some suggestions offered. Are you saying, or would you be able to state for the record, that you'd like things to remain status quo, as it relates to PIPEDA, on this issue of the duty to notify?

● (1015)

Mr. Robert Kimball: Thank you for the question.

Yes, we would like things to remain, but I'll back up and qualify this.

As insurance brokers, we look to try to protect our clients. If there is a breach to any of our clients, we certainly want to make sure that they are well aware of it. British Columbia currently, I believe, has something that is very workable. What they're saying there is they want to be able to assess what the breach was, find out who was affected, make sure they contact those affected people, and learn about and mitigate any possibility of these breaches continuing in the future.

We find that to be a good common sense approach. Certainly if people's information has been breached, absolutely the insurance brokers across Canada want to make sure those people are made aware of the breach and are able to handle it in the most appropriate way.

We do not feel that it may be in the best interest to worry all of your clients if, for instance, you happen to have a rock thrown through the front window of your business and it sets off your alarm and there was absolutely no breach into your office. You wouldn't notify all those clients and unduly worry them. If there was an actual possibility that information got out, insurance brokers around Canada would want to make sure that those affected clients were definitely notified. We're very pro that.

Mr. Bruce Stanton: Would you then say that this approach taken by B.C. that leaves this really in the hands, in your case, of the broker, but let's say of the business that's so affected, and that places the onus on them to do the assessment, determine who was affected by this breach, and then implement some notification procedure would be quite acceptable and quite workable?

Mr. Robert Kimball: Our understanding is that it would probably be best. The business would probably have the best handle on who was affected and what the effect was.

As I said before, our business is protection of our clients. We do it in every policy we have out there. Their privacy is absolutely no different, so we would want to make sure those people were made aware. We feel that's probably the best place to leave it.

Mr. Bruce Stanton: Just to finish up on that point, it would appear currently in PIPEDA that there isn't really a direction or a model or a suggested procedure for these kinds of situations. There is extensive verbiage around where disclosure can be provided without consent and so on, but we don't really set that out. At least, I've scanned through and I can't locate anything in terms of pointing to any specific language in PIPEDA that really talks about this duty to notify, from what I could see.

What you're suggesting here and what other witnesses have suggested would in fact be an addition either in schedule 1 or in the act itself to provide some guidance for these types of circumstances.

Would that be your summation?

Mr. Robert Kimball: I'll ask Mr. Masnyk if he could speak to that.

Mr. Steve Masnyk: I think the wording found in the B.C. model is—how can I put it?—probably the least offensive.

Mr. Bruce Stanton: It would be the least offensive to whom?

Mr. Steve Masnyk: Well, by “least offensive” I mean that we could actually implement on a practical basis.

Mr. Bruce Stanton: Okay, very good.

Thank you very much.

Do I have more time, Mr. Chairman?

The Chair: No.

Thank you.

We'll go to Mr. Pearson, followed by Mr. Van Kesteren and Mr. Peterson. The final questioner I have on the list is Mr. Tilson.

Mr. Glen Pearson (London North Centre, Lib.): Thank you, Mr. Chair.

My question is for Ms. Gray-Donald. We talked about smaller ISPs. When Mr. Sullivan was talking, he said that the larger ones, primarily, tend to comply with what's going on. Have the smaller ones been resistant to that in large numbers, or is it just...?

● (1020)

Mrs. Krista Gray-Donald: As my colleague had indicated, it's really hard to answer that question. If an ISP refuses to cooperate, in many cases, an investigation cannot be completed. There's no chance to find the evidence because it does move so quickly.

It has been our experience, through anecdotal reports from law enforcement, that by and large these smaller ISPs are resistant to cooperating.

Mr. Glen Pearson: Right.

Can you give me an indication of the rate of increase of the smaller ISPs? You once again referred to more cropping up all the time. Do you have any idea?

Mrs. Krista Gray-Donald: In terms of actual numbers, we're starting to gather some data on contact information for the smaller ISPs to address this issue, but we don't have any hard and fast numbers as to how many there are. I know if you do a Google search and say, "Internet service provider Ottawa", you will end up with a lot more than Rogers and Bell. So there are quite a number.

Mr. Glen Pearson: It would seem to me that there would be an alarming increase. Is that correct?

Mrs. Krista Gray-Donald: Yes.

Mr. Glen Pearson: Mr. Sullivan, I was a firefighter for 30 years, in a previous life, before I came here. In the last couple of years, we cooperated with the police on the issue of cellphones with cameras. The phones were captured because of a fire. We went in there. The police went in there and found these cellphones that had pictures of children on them.

Is that a special challenge to you? Outside of the regular stuff over the Internet, is the giving out of information over cellphones back and forth so quickly a special challenge? Or does that still fall within the regular framework?

Mr. Steve Sullivan: I don't pretend to be an expert on it. But I can say that the advancement of technology is becoming an increasing issue for law enforcement in a very general sense, not just related to this issue, but with all the BlackBerrys, ISPs, and cellphones....

The technology is advancing so fast, and I think that as good a job as our law enforcement is doing, they're still playing catch-up. And they have a way to go to make sure they're on par with the people who use the technology for a purpose it's not intended for. I can't speak to it specifically, but in general, I think cellphones and increased technology are an issue for law enforcement.

Mr. Glen Pearson: It seems to me, at least in the cases I was involved with, that police are having a dickens of a time following these cellphone pictures going across, as they were, as opposed to Internet things that people are looking at on a computer. Is that correct? Is it more difficult?

A witness: [*Inaudible—Editor*]

Mr. Glen Pearson: Okay. Thank you.

This is my final question. Do you have a jurisdiction you would point us to, some area, where they have a model that you think would be wise for us to follow, whether it's another country or in Europe or whatever?

Mr. Steve Sullivan: I know that there are other jurisdictions that do require ISPs to do more and to cooperate with these kinds of things. The United States has legislation. The United Kingdom and Australia have legislation. We found that out when we were looking at Bill C-74, the bill from the previous government to require ISPs.... But this is done in other jurisdictions. It has been going on for quite some time.

Mr. Glen Pearson: It is done to a greater or lesser degree. But is there one that you would see as a good model for us?

Mr. Steve Sullivan: We haven't studied the models in depth, so I can't give you any specifics.

Mr. Glen Pearson: That's good.

Thank you, Mr. Chair.

Mr. Steve Sullivan: Mr. Chair, I did find the copy of the letter from the Privacy Commissioner. We could have it photocopied, perhaps, before we leave.

The Chair: You can deal with the clerk on that. But we'd be interested in having a copy.

Mr. Pearson, I think I'll ask the researcher to have a copy of Bill C-74 made available for each member of the committee for consideration when we're considering our draft report. The issue was dealt with in some manner in that report, and the witnesses have mentioned it on numerous occasions. We'll take a look at that just to see what that approach was and whether the committee would be interested in considering it.

It's also a question that some members might want to put to the minister, when the minister comes, to determine whether the minister has an opinion on Bill C-74 or any portion of it that might be relevant to our inquiry. That's just a heads-up for members.

We'll have Mr. Van Kesteren and then Mr. Peterson.

Mr. Dave Van Kesteren (Chatham-Kent—Essex, CPC): Thank you, Mr. Chair, and thank you all for coming.

Mr. Sullivan, I think that may have been the most disturbing thing I've ever heard, and I'm not reprimanding you; I think we need to hear that stuff. That is just so vile, and I really have a hard time. I know we're frustrated with combating this, but calling that privacy rights is such a violation. It should be addressed in our Criminal Code. We have to stamp this out. I commend you for doing that.

I say that because I have two sons who are policemen. One of them is on a SERT team. One of the things that really concerns me is their discouragement, especially the longer they're in police work, with things like SIU and some of the restraints put around police today. We hear about all the abuses, but I don't think too many people have really walked the beat with what they're coming up against, child pornography being one of those things.

I really have nothing to ask the insurance people. I commend you people. I think you've done a good job with privacy. As I've said before, you could have written the book. PIPEDA makes sense in your business, and you have to continue along that path; it's the way that's going to keep you in business.

For policing, I need to ask you this question: does PIPEDA hinder your police work? I know these bodies are there for a purpose, like SIU, but does PIPEDA hinder you in what you have to do? Be blunt.

● (1025)

Mr. Clayton Pecknold: I've been listening to the line of questions and the answers. If you'll permit me, I'll answer that question in a couple of ways.

First of all, I will say that the misinterpretation of PIPEDA and perhaps the ambiguity of the act does on occasion hinder us, yes. Specifically, if you like, we can put some information before this committee in pretty short order from the various child pornography sections.

Angie Howe was mentioned. She presented on Bill C-2. She's a detective superintendent with the OPP. We can have her put together some information specifically on some specific problems we're dealing with in child exploitation, if it would be of assistance, Mr. Chair. We can put that before you in writing.

The Chair: Mr. Pecknold, if you can relate it to how PIPEDA specifically is impeding investigations, that would be helpful.

Mr. Clayton Pecknold: Sure. I'll endeavour to do that when I leave here.

The second point is we talked a little bit about, and I think the honourable member over here mentioned, cellphone usage. This technology advancement is a real issue for us. The lawful access issues are a number one priority for the CACP. With respect to electronic interception of communications, we are dealing with laws written in 1974, when we had rotary phones. I have a BlackBerry on my hip, and we all have satellite phones.

We are losing the race in terms of technology and interception and investigation of serious offences—organized crime offences, national security offences. We're losing the race technologically. We have been pushing government to put this bill forward and we're hoping they'll put it forward. I did not come here intending to speak to this at this committee, but I can see it has touched on it.

I will say that on the technology side, yes, we are hindered. PIPEDA doesn't address that necessarily, but if PIPEDA can address the difficulty that some in the private sector have in complying with the lawful authority of the police, then I would encourage this committee to try to address that.

Mr. Steve Sullivan: I will just restate again that certainly we've heard anecdotal information from law enforcement that...my friend is correct: the misinterpretation of the legislation—because there is some room for interpretation—has hindered law enforcement.

Our position is that even if 99% of the ISPs cooperate and 1% don't, it's not good enough. If there's one child out there who's left behind, left to be abused, left to have their images used when we could be stopping it or trying to stop it, then we need to do more.

The Chair: Thank you.

Mr. Peterson is next. He will be followed by Mr. Tilson. If any other members want to ask questions, just catch the eye of the clerk and he'll put your name down.

Hon. Jim Peterson: Ms. Gray-Donald, did I hear you say that by and large small ISPs refuse to cooperate with the police?

Mrs. Krista Gray-Donald: That is the information we have from anecdotal police reporting through investigations. By and large, it is open to interpretation. To clarify, they are more frequently cited as those that don't cooperate.

Hon. Jim Peterson: By and large, it would connote to me 50% or more of non-cooperation.

Mrs. Krista Gray-Donald: I can't put a figure on it, so I would like to clarify and say that isn't it.

Hon. Jim Peterson: Are you asking for this power, that an ISP must provide personal information, just for crimes against children or for all types of police investigations?

● (1030)

Mr. Steve Sullivan: Our focus here today is crimes against children. Having said that, I think it's appropriate that we look at other issues that are identified. Again, Bill C-74 speaks to the broader issue. Our issue to raise here today is the sexual exploitation of children. That's not to say there shouldn't be other issues, but that's the issue that concerns us the most at this time.

Hon. Jim Peterson: But there are lots of crimes that are heinous.

Mr. Steve Sullivan: Absolutely.

Hon. Jim Peterson: In some cases, for example, police will need a warrant if they're going to search a premise or get information. Are you saying they shouldn't have to get a warrant just if they're dealing with an ISP, or if they're dealing with anybody?

Mr. Steve Sullivan: We're saying they shouldn't have to get a warrant to get a name and address of someone who's suspected of trading child pornography or distributing child pornography. They shouldn't have to get a warrant for that information. As my friend mentioned, it's not about the websites they visit, their e-mails; it's their name and their address.

Hon. Jim Peterson: Do you know if Bill C-74 limits it to child abuse, or is it all sorts of crime?

Mr. Steve Sullivan: It's all sorts of crime.

Hon. Jim Peterson: Thank you.

The Chair: Thank you, Mr. Peterson.

I call on Mr. Tilson now, and I'd like to thank Mr. Tilson for chairing the committee last week. Thank you very much.

Mr. David Tilson: Mr. Chairman, thank you.

Mr. Peterson has pretty well asked my question. I have to say I congratulate the police for the work they do on this issue, and your organization as well, Mr. Sullivan. I understand the frustrations that the police particularly have in making investigations because of the restrictions that are put against you, hindering your investigations. I understand that.

I'm going to zero in on a question that has been pretty well asked several times. It's the issue of there not being a warrant, the lack of requirement for a warrant. I'd like to raise the issue of where there have been false accusations, abuse of process, oversight, and maybe there are other examples. The question was asked whether you had a proposed amendment, and I understand it's a tricky thing. We need all the help we can get, quite frankly.

My question is to both Mr. Sullivan and Mr. Pecknold. If you're not going to have to have a warrant in restricted situations, should there be some threshold? Otherwise, and I'm not casting aspersions on anyone, there could be an abuse with this not requiring a warrant. I understand your frustrations, particularly the police, but it can be dangerous.

Mr. Pecknold.

Mr. Clayton Pecknold: Thank you for the opportunity to respond to that. Perhaps I'll try to provide some clarity of our view on that.

Our view is that whenever information is of the type that attracts section 8 of the charter protection, the right to privacy protection, or the right to be free from unreasonable search and seizure, the Supreme Court of Canada has clearly stated that the police require a warrant; they require prior judicial authorization. It gives guidance in Hunter v. Southam; it gives guidance on what type of information it is.

What we are talking about here is access to information that does not attract that threshold, so the threshold is built in. We don't require a warrant for information on customers' names and addresses. That threshold is not there. The courts have said we don't need a warrant to get that information.

This is not a case of people's bank records, how much money they earn, or what their sexual preferences are. We absolutely require warrants for those things and will continue to require them. Otherwise the information is not admissible in court, in any event. So we're under the supervision of the court, and those protections are built in. It's clearly not our position that in this bill or any other bill we should be given the authority to access information of that nature without a warrant. We don't believe that. It's just not the way the law is in Canada, and we accept that.

What we're talking about in this case, for example, is our ability to go to a bank or an ISP and ask whether so-and-so is a customer, and whether he has an account there, yes or no. Then we carry out the investigation. That's the type of information we're seeking to have released to us.

As to my friend's discussion about a positive obligation to disclose things with respect to child pornography, we haven't put our minds to that, but it's certainly an area that this committee may wish to consider—a positive obligation on ISPs—but that would be a private duty.

● (1035)

Mr. Steve Sullivan: I don't think Parliament intended for police to get a warrant when they passed this legislation. I think they put in the first clause “if you have a warrant”...in other words, if you have lawful authority. I don't think Parliament intended for that to mean a warrant. I think it was left sort of ambiguous, so it has been interpreted by some to suggest you need a warrant.

Again, as my friend suggested, you're really looking at someone's name and address, perhaps. You can get that off their licence plate. You can stop someone on the street and ask them to identify themselves. You don't need warrants for those things. So I think the protections are built in to the process now.

Mr. David Tilson: We have only a few more witnesses left in our hearings. Then we'll hear from the commissioner and the minister, and then we'll prepare a report.

I know you haven't prepared a proposed amendment, but it's an interesting issue. It would be interesting for our consideration if you could address that, if possible. If not, I'm sure we will consider it ourselves.

Thank you.

The Chair: Thank you, Mr. Tilson.

Mr. Dhaliwal.

Mr. Sukh Dhaliwal: My question or comment is to the insurance fellows here. We are hearing about this work product definition at almost every meeting, and we want to fix it once and for all, for all the industries.

IMS brought in a definition. Have you gone through that? Have you looked at the presentation they made to the committee earlier?

Mr. Steve Masnyk: We're not aware of any IMS definition.

Mr. Sukh Dhaliwal: They brought in a definition.

We'll be getting into a challenge because small businesses have their own issues compared to bigger businesses. I wonder if you could come up with some suggestions and send them to us so we can fix it once and for all.

The Chair: I wasn't here, but I believe they gave a recommended definition. Maybe you'd like to take a look at the evidence and offer your comments, since the definition of work product was point two of your three points, and whether you agree, disagree, or have some suggestions on how to change it.

Mr. Steve Masnyk: Has that been tabled with the committee?

The Chair: Yes.

Mr. Steve Masnyk: So we can get it from you.

The Chair: I imagine the clerk will be able to help you out in that regard.

Mr. Steve Masnyk: We'll respond back with our comments.

The Chair: Is that it, Mr. Dhaliwal?

Mr. Sukh Dhaliwal: Yes, thank you.

The Chair: I want to remind committee members that Thursday we have the Canadian Federation of Independent Business and the Consumers' Association. Next Tuesday we have the RCMP. It's a late addition, but they've urgently requested that they appear.

On Thursday next week we have the Privacy Commissioner. On Tuesday of the following week, February 27, we will begin our deliberations, because the minister is not available to meet with us until March 1. It might not be a bad idea if we begin our deliberations on the Tuesday so we can focus on the kinds of questions we want to ask the minister on Thursday, March 1. That will be our last meeting until after the two-week break.

To our witnesses, thank you very much for appearing before us today, answering our questions, and trying to help us in our deliberations on this very interesting statute.

The researcher wants me to remind everyone that a summary of recommendations from all our witnesses will come out to all of us prior to the beginning of our deliberations on February 27.

Once again, thanks to you all. Amazingly, we have 20 minutes to get to our next committees.

I adjourn the meeting.

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

The Speaker of the House hereby grants permission to reproduce this document, in whole or in part, for use in schools and for other purposes such as private study, research, criticism, review or newspaper summary. Any commercial or other use or reproduction of this publication requires the express prior written authorization of the Speaker of the House of Commons.

Le Président de la Chambre des communes accorde, par la présente, l'autorisation de reproduire la totalité ou une partie de ce document à des fins éducatives et à des fins d'étude privée, de recherche, de critique, de compte rendu ou en vue d'en préparer un résumé de journal. Toute reproduction de ce document à des fins commerciales ou autres nécessite l'obtention au préalable d'une autorisation écrite du Président.