

House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) - Meeting, Feb. 13, 2007 (Chaired by Tom Wappel)

Notes taken by Tara Berish, CIPPIC Articling Student

**NB: This is not a transcript. We do not guarantee accuracy of these meeting notes. For a transcript of the meeting, see the Committee website.

Witnesses

- Canadian Resource Centre for Victims of Crime
 - Steve Sullivan, President
 - Krista Gray-Donald, Director of Research
- Insurance Brokers Association of Canada
 - Robert Kimball, Chairman
 - Peter Fredericks, Vice-President
 - Steve Masnyk, Manager of Communications
- Canadian Association of Chiefs of Police
 - Clayton J.D. Pecknold, Co-Chair, Law Amendments Committee

Steve Sullivan, President, Canadian Resource Centre for Victims of Crime

- Advocacy group
- Raise issues with all levels of gov't advocating on behalf of victims
- Internet child exploitation
- Funded by police association
- Impact of PIPEDA on law enforcement efforts to address these issues
- Confusion as to whether ISPs can or should provide info to police for law enforcement efforts – they should be able to share, there shouldn't be any discretion
- The images are getting more violent, and the children are getting younger
- Can you imagine a bigger violation of your privacy than that? Nobody's speaking for the children.
- Case by case basis isn't good enough.
- Need to balance the privacy rights of children with those of Internet users
- S. 3 – when organization may disclose personal info – with a warrant, request by gov't inst. with lawful authority – what does this second point mean? Can we clarify that?
- Should have investigators come and talk about their experiences. Many larger ISPs cooperate without a warrant, but not all of them do.
- Why don't they just get a warrant? Sometimes there isn't time
- They're just asking for names and addresses, shouldn't need a warrant for this.
- There shouldn't be any discretion for ISPs to help in these cases, but at least should clarify these provisions
- Costs to companies – there should be a duty to cooperate. There are consequences to these things.
- Encourage the Privacy Commissioner to take a more active role in this area.

Robert Kimball, Chairman, Insurance Brokers Association of Canada

- Small town insurance broker
- 6 people in his firm
- family business
- providing with an industry and personal perspective on this
- privacy important, and should never be compromised, need safeguards to protect from privacy abuses
- general effectiveness of PIPEDA – it works and works well
- haven't received a single complaint re: privacy since PIPEDA
- approach taken re: spirit and intention of PIPEDA is right
- guide of implementation was distributed, also seminars and roadshows
- brokers have embraced the guidelines as part of their everyday business
- they have long-term employees
- small town, so privacy very important
- computer privacy – passwords etc.

Peter Fredericks, Vice-President, Insurance Brokers Association of Canada

- Broker in a small town in N.S.
- Two issues: the goal/mandate of the OPC – the ombuds model is good. Work product needs clarification – widely believed that info obtained in the course of business is proprietary to the firm.
- Notice of breach – our basic reason for being is to protect our clients. It's good business for us to notify our clients of breach. But, it's not easy to regulate this.

Clayton J.D. Pecknold, Co-Chair, Law Amendments Committee, Canadian Association of Chiefs of Police

- Membership of the org.
- Police community is concerned about privacy of Canadians – work hard to comply with their privacy requirements
- Internet child pornography is a concern
- Want balance and restraint, but also tools to investigate these crimes
- Primary duty of a police officer is protection and keeping the peace
- Need timely access to info about an individual in order to help them achieve their goals
- Digital age poses challenges to effective policing
- Police operate under the scrutiny of the courts and public
- Many everyday functions of the police do not involve their criminal powers
- Disclosure to police without consent, and...
- Police often need to seek info without a warrant
- Sometimes the info sought does not attract s. 8 Charter protection, or can be in the early stages of a missing person investigation – for this we rely on s. 7(3.1)
- It's overly restrictive, and defeats the intent of the provision
- Police are careful to not jeopardize prosecution by collecting evidence wrong
- Protection is only triggered when a person makes the request...

- Clarify the ambiguity in s. 7 and 9, clarify the term lawful authority, which would clearly show that a warrant is not required
- S. 9 – amendment should be made to prohibit disclosure that the police have made a request for information
- Police work closely with all members of the community

Comments and Frequently Asked Questions:

- It took a while for MPs to start asking about the possible abuses related to requiring ISPs to turn over information to police without a warrant, but they eventually did.
- People discussing child sexual exploitation on the Internet took an odd view of warrants and the Charter, arguing that receiving names and addresses from an ISP without a warrant would not infringe on Charter rights since information on one's actual activities would not be collected.
- The Insurance Brokers Association of Canada did not really say anything that other insurers had not already said.

Questions and Answers

Chair: Has the phrase “lawful authority” been interpreted by a higher court?

Pecknold: I don't think so.

Dhaliwal: Are there any ISPs that are not cooperating, and what are the circumstances?

Sullivan: Most of the bigger ones are, but it happens on a case by case basis. Some smaller ISPs that exist only to trade in child sexual abuse, they don't cooperate.

Dhaliwal: You said something about costs?

Sullivan: There was a case in Toronto – there was a homicide investigation – and the ISP said that cooperating with law enforcement would be a financial burden. The complete annual cost would be 600,000\$, but the forensic auditor said it was .000X % of their operating costs. I think ideally we would like ISPs to take a more active role to make sure that their services are not being used to exploit children – we're not asking them to police all the time, but if they become aware...

Pecknold: The ongoing lawful access issues. The TELUS mobility case – dealt with idea of fee for complying with the protection of information. Deregulation of telecoms has had an effect on the industry. They're good corporate citizens, and they want to comply, but find it hard. We try to give them some comfort and clarity as to what's involved. We run into some problems. Sometimes data needs to be gotten too quickly.

Vincent: You want ISPs to give out info when?

Sullivan: They have the discretion to give out the info. We want to clear up that confusion.

Vincent: But you want them to divulge the info to investigators? Investigators could be anyone – insurance companies etc.

Sullivan: Our interest is ISPs, because that's where the children are being exploited... we think that when the police ask them for info, they should comply, there should not be discretion. That was what previous legislation was asking for.

Vincent: Do you want this to apply to everyone, or just the internet?

Sullivan: Our experience is only related to the internet.

Vincent: Don't you think police could abuse this power?

Pecknold: Let me clarify the type of info we're talking about – name and address, not internet usage etc. We're looking for X, is X one of your customers. That allows police to get the information through a warrant. It's limiting to not be allowed to know whether there's a customer there. We're certainly not going to read peoples' emails.

Vincent: If you lose info in the insurance business, you want it be your own business to decide whether to notify your clients or not?

Kimball: We've never had an incident. We believe that if there is a file lost, we should protect our clients, and inform them, and learn from it. We don't want to have to worry all of the clients if one file was lost – if there was no worry of breach to them.

Vincent: But what is your interpretation of risk? How do you determine what the risk is?

Kimball: Again, I have no experience at this, and most do not. We have regular protection at the office to protect against breach. We don't collect much information in our offices – ie, no SIN. If something happened, we would let our clients know, and work with them to reduce possible harm.

Chair: Lawful authority - are you concerned with the word “may” – disclose to conform with the requirements of the schema. “May” is a common drafting term. It seems to me that if there's a subpoena or warrant, there should be no discretion.

Pecknold: I hadn't noticed that, but in our view, a court order is must. Brings back the Telus Mobility case. If the legislation doesn't provide for a fee, there is no fee.

Chair: The way I read it, “may” means “is permitted”.

Wallace: Insurance group – you talked about work product which is unclear in this legislation. Do you have a definition with you, and changes to the wording you'd like to see?

Fredericks: No – we're just looking at proprietary information. Information about your home – those are yours, you would get them back. But, if I use a calculator to determine the value of your home, I want to be able to keep the results of those calculations, not have you take them with you to another broker.

Wallace: Notification – it should be narrowed to those who are directly affected?

Answer: Absolutely

Wallace: Do you have a new definition for lawful authority?

Pecknold: No, I haven't put my mind to it, but the key is clarity.

Wallace: Prohibition of disclosure to police – you want the wording changed to show they have no choice but to disclose to the police, and then the police have the discretion of deciding whether this fact should be disclosed?

Pecknold: Well, the Privacy Commissioner should decide...

Wallace: you're interested in a better definition of lawful authority. You'd like to see something in the preamble about working with the police?

Sullivan: We'd like to see some sort of indication that PIPEDA was never intended to hinder the police. Children have a right to privacy, especially re: their sexual exploitation.

Wallace: I have a private members bill which allows a loved one to bring in a DNA sample to help find a missing person. There is one small issue about privacy that the

person has not consented to their DNA being reviewed. What would the victims say about this?

Sullivan: we did a study on families and homicides – the toll on parents is tremendous. There were privacy concerns raised – those are fair concerns (kids fleeing from dangerous families). I think there's a way to balance those privacy interests – if the police find someone who left on purpose, there are ways of dealing with it. The comfort of a family knowing is important.

Chair: ... something about disclosure to investigators etc.

Peterson: PIPEDA uses the word “may”; you would want “must”? If there's not a warrant – could you give us some wording?

Sullivan: From our perspective, in this context of child porn it should be must...

Peterson:...

Sullivan: Anecdotal evidence – if we don't get the name and address, the investigation's over and we can't go on.

Peterson: You want the Privacy Commissioner to take a bigger role in tracking down users – what role would this be?

Sullivan: Not in actually tracking down, but in deciding what ISPs could do to remove the images. She doesn't have a law enforcement role, but she is an advocate for privacy rights. We have a victim impact statement, and one of the hardest parts for the victim is knowing that her info is still out there – we want the commissioner to speak for this girl.

Peterson – But how do you retrieve these things once they're out there?

Sullivan: You don't, but...

Reid: When discussing child porn, we're really dealing with two distinct offences, one which is the original thing (rape), the other is the distribution of the images after the fact. Robbery is distinct from possession of stolen property after the offence. If the second offence is treated as a form of stolen property, there is a logical way of dealing with this. If we use the pawn shop as analogy to an ISP, is there some way of addressing this in the law?

Sullivan: There are jurisdictions where pawn shops are obliged to track... the difference is that to us the simple possession of photos is a form of abuse. Some offenders use them to break down the barriers of children.

Reid – That would seem to be a separate offence...

Gray-Donald: in Gatineau – they got a call, could investigate...

Reid: Assuming that the offence is still ongoing, then getting the info could help you in tracing it back, right?

Sullivan: There is a lot of work being done by law enforcement to track back, identify the kids and rescue them.

Bonsant: I understand what you're trying to do, but the problem is not just Canada, it's international. I think your question isn't limited to the internet. Good luck on that. On the level of collecting people who make the porn, we get... but what happens with the clients?

Sullivan: I agree with you that this is an int'l problem. Some countries don't do very much. We're interested in doing more than just catching bad guys. Are there ways that ISPs could at least take images off their own sites and networks?

Bonsant: I was on the Arar commission – I had some difficulties re: privacy. I think there are police who do a great job, but not everyone. There was information which was invented – that's what worries me. If we give them an exception, there will be abuses. I know this sounds like an exaggeration, but we have to be very careful. We have to be very careful when we ask for information from people.

Pecknold: I don't believe that any of the information in the Commission was manufactured. In any event, there are a number of mechanisms for us in place to deal with breaches of policies and laws – I myself have prosecuted officers for breaches of privacy. But there's also a need to get the information to protect people.

Chair: Could we focus on PIPEDA?

Stanton: Insurance brokers – the 3rd item that you talked about – duty to notify. That issue has been in the news. You said this would be problematic to regulate. Could you expand? Would you like things to remain status quo?

Kimbal: Yes we would like things to... we want to protect our clients – if there's a breach, we want them to know. BC has something which is workable. They want to be able to assess what the breach was... we think that's a good common sense approach. Certainly if there's a breach, we should let people know – but we don't think it's a good idea to worry everyone if there hasn't been a real breach.

Stanton: So, would you say that this approach taken by BC leaves us in the hands of the broker – that this would be acceptable?

Kimball: That would be best – we know what the business is, who our clients are.

Stanton: In PIPEDA, there isn't a procedure, model etc for these cases. There's a rule, but they don't really set that out. So what you're suggesting would be in addition to what's already there?

Masnyk: I think the wording in the BC model would be the least offensive we could actually implement.

Question: Larger ISPs tend to comply, but are the smaller ones resistant in large numbers?

Gray-Donald: My colleague showed that it's hard to find out in large numbers...

Question: What's the rate of... ISPs?

Gray-Donald: We don't have any hard or fast numbers...

Question: We cooperated with police on issues of cell phones in fires. Pictures of children on cell phones, giving out of info over cell phones – is that a concern?

Sullivan: I'm not an expert, but the advancement of technology is an issue for law enforcement, it's advancing so fast.

Question: Police are having a dickens of a time following these cell phone things. Do you have a jurisdiction we should follow?

Sullivan: US, Aust, UK all have legislation. This is going on in other jurisdictions. We haven't studied the models in depth.

Van Kesteren: Sullivan – that is the most disturbing thing I’ve ever heard. That is such a violation of privacy rights. I have two sons, and one of the things that discourages them is the difficulties in police work. Does PIPEDA hinder police work?

Pecknold: The misinterpretation of PIPEDA, and its ambiguity does sometimes hinder police work... we can have someone put together specific info on the investigation of these things.

Chair: Can we relate it to PIPEDA?

Pecknold: Sure – the cell phone technology thing – we’re dealing with laws of a long time ago... we’re losing the race technologically. I will say that on the tech side, yes we’re hindered – PIPEDA doesn’t address that. But...

Sullivan: I agree that misinterpretation has hindered law enforcement – if even 1% of ISPs don’t cooperate, it’s too many.

Peterson: By and large, small ISPs have refused to cooperate with police?

Gray-Donald: That’s what we are seeing – I can’t put a figure on it.

Peterson: Are you asking for the power that an ISP must provide personal info just for crimes against children or all investigations?

Sullivan: We are here re: sexual exploitation of children

Peterson: But there are lots of crimes which are heinous. They shouldn’t have to get a warrant for an ISP, or for everyone?

Sullivan: For collection of name and address.

Tilson: Peterson has asked my question. Lack of requirement of a warrant – false accusations, abuse of process, oversight... You need all the help you can get. If you’re not going to have to have a warrant – shouldn’t there be some threshold? I’m not casting aspersions on anyone, but there could be an abuse. I understand your frustrations, but it could be dangerous.

Pecknold: whenever info is of a nature that could attract Charter protection, the SCC says you need a warrant. But we’re talking about info which does not meet that threshold. We’re just asking for name and address. Those protections are built in. It’s our view that we should be given access to that information without a warrant – just ask if someone is a customer. Should there be a positive obligation on ISPs to disclose in cases of child porn – committee could look at that.

Dhaliwal: Work product – we want to fix it once and for all for all industries – have you gone through IMS’s definition and looked at it?

Answer: We’re not aware of their def.

Dhaliwal: Can you give us a recommendation to fix this once and for all?

Answer: Ok

Chair: Why don’t you look at their definition, and then give us your opinion.

End of Meeting