

House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) - Meeting, Feb. 20, 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

Royal Canadian Mounted Police

- Bruce Rogerson, Assistant Commissioner
- Art Crockett, Officer in Charge, Strategic Services Branch, Technical Operations;
- Earla-Kim McColl, Officer in Charge, National Child Exploitation Coordination Centre.

Bruce Rogerson, Royal Canadian Mounted Police, Assistant Commissioner

- Prior to 5 years ago, we were able to collect all kinds of info from organizations without complaint
- We get along with the community – people trust us
- There's confusion now, when we ask people for info – it's like gathering a 1000 piece puzzle – we don't really know what's happening when we gather it
- S. 7 and 9 PIPEDA – confusing
- S. 7 – lawful authority – court order, docs – orgs have refused to provide simple things which used to be provided before
- St. Thomas – ISP provided info without a warrant, so the police were able to gather enough info to get a warrant to get someone who was assaulting a young lady
- Warrant – there's case law whereby the info sought under PIPEDA doesn't warrant a search warrant – name and address info is not considered a violation of rights under the Charter
- We take on the risk if we use or misuse the info
- We'd like the lawful authority provision to be redefined – make it clear we can get these things without a court order
- If we access someone's name, we don't want that to be disclosed to them – we want PIPEDA to reflect that
- S. 7 and 9
- RCMP Act – governs privacy, and we can be fined or dismissed for not abiding by it
- We have the Criminal Code for abuse of process etc
- Public Complaints Commission – people can use that to make complaints against us

My Comments and Frequently Asked Questions

- Perhaps an indication that these meetings have been running for some time now, the discussion has become frequently tangential, if not off-topic altogether. However, the main points to come out of this meeting are:
 - 1) The RCMP would like to retain the power to obtain information from businesses, without a warrant. They argue that this information would be

limited to names and addresses, and is necessary to help them obtain a warrant for deeper investigation.

- 2) The RCMP would also like PIPEDA to specify that such requests may not be disclosed to the person about whom the request is made, without the RCMP's consent.
- The RCMP believes that PIPEDA allows for the above, but that businesses are risk-averse, and so will not disclose information without a court order.
- Martin brought up the Public Safety Act again.

Questions and Answers

Dhaliwal: I certainly agree with you on the ISP providers - without the information, there could be child abuse. But, with respect to the public not knowing that an investigation is going on...aren't there cases where the public would have access?

Rogerson: If you're talking about open source information, you're right... With respect to the exchange of info between CSIS and the RCMP – CSIS collects info in an informal way, not national info. When it comes to national security, we share info. We have an excellent relationship with CSIS for the exchange of info which helps them do their job. They're national intelligence – we're enforcement, governed by the Criminal Code.

Dhaliwal: Do you think it's in the best interest for the public to know through access to information when there's an investigation going on?

Rogerson: In reality, we are the public's interest. We're accessing info under lawful authority based on the Criminal Code. The general public are not held up to the same level of scrutiny as we are.

Dhaliwal...

Rogerson: I've not really seen breaches. The justice system determines which evidence gets thrown out – and they will throw out info if it gets collected inappropriately. So, we have a watchdog. The info we gather informally allows us to develop our info enough to get a warrant. [Gave examples of where this is necessary] If we have no grounds for a search warrant, we have to get them.

Vincent: You're giving very clear examples. But, you're giving us the sympathetic examples. But, this opens the door to everything. I think it's a little too much. You could be sharing info with everyone. There are some holes here. Apart from internal disciplinary measures, do you have any other measures to make sure you don't share the info etc.? What do you expect to do to better protect this info?

Rogerson: We have something that we've just passed around to control this. As you know, in Montreal... we have rules to control this stuff. But from time to time, this info is needed.

Vincent: But don't you think that the police can just go around and ask for everyone's name? You're saying that they can't disclose to the person whose info you collected that you did so? But if you go get someone's name, you have a reason. It's not just for fun.

Crockett: The information we're asking for is basic – not core info about an individual. For instance, we arrive and see there's a dead body in the hotel – we ask who was in the hotel. So we could question them. That doesn't seem personal to us. Or to Canadians. It's my experience that the public and private sector want to help and get involved, but

they're not sure they're allowed. We want them to be protected, it's up to us to protect what we do with that info.

Martin: It's my impression that PIPEDA allows you to use that info already. My understanding is that the change which came about in the Public Safety Act, would allow organizations to go out and actually collect info for the RCMP. That's what's chilling to me – the individual concerned might never know that their fundamental rights to privacy could be violated by a private organization, and then there would be no redress the way there would be in the public. I think this is an end run of the Charter. This is cited for sketchy reasons – not just pedophilia, but national security and the conduct of international affairs – that's so wide and abstract it could be almost anything.

McColl: PIPEDA has affected what we are able to do on a daily basis. The amendments to PIPEDA haven't changed us. All we want is clarification. Anything that requires Charter protection is governed by the courts – they will ensure that there's protection.

Martin: I understand that. Currently, information can't be shared in certain ways. But the idea that private organizations can not only share info, but go out and collect it... maybe you didn't know that.

Bruce: ...

Martin: This is deputizing the private sector to do your work.

Rogerson: On a daily basis, people have this information, and ... I will say that we've used our technology to help identify hostages in Iraq. Also, for reasons of economic integrity. So, we do help Industry.

Chair: So, what are the purposes for which you're appearing? Lawful authority should be amended so that it's clear that a warrant isn't required. Is that what you're saying? Term "lawful authority" is not defined in the Act.

Rogerson: Yes

Chair: S. 9 – if a person calls up my bank, and asks if the police contacted the bank about that person's info – then the bank has to call you to find out if it's ok to answer your question? You have a concern with disclosing... before the client is advised about the police action, the police should be advised. Is that correct?

Rogerson: Yes

Chair: 2nd portion, as I understand it, you want to have a blanket ability to object under all circumstances?

Bruce: Yes

Stanton: Which provisions was Martin citing?

Chair: 7.3....

Martin: Also, 7.3.d.ii

Stanton: Can you think of some other information which helps in the investigation that is quite normal in the general process of enforcement activities?

[inaudible exchange between Stanton and Rogerson]

McColl: Under the CC, we have information about individuals – that's what we do, we gather info about individuals to decide whether an investigation is warranted or not.

Crockett:...

Stanton: There are numerous examples where legislation permits the collection of info for investigation. In s. 7, specifically talking about the fact that an organization... under 7(3)

an organization may disclose info without consent – the debate seems to turn on the word “may”. The discretion is left to the organization. Has that been a problem for you in your investigations?

McColl: That has been a great obstacle for us. Interpretation of “lawful authority” and interpretation of [inaudible] – those are the problems. In our line of work, most of the requests from ISPs are refused under PIPEDA. If we can’t get the little bit of info, we can’t start an investigation, this is the single largest impediment to our work today.

Stanton: It would appear that even in the case of 7(3)(c) – the override stills says “may”. How do you get around that?

McColl: What we’re talking about is info that is pre-warrant – you can’t get a warrant for it.

Dhaliwal: If the RCMP is investigating a person’s bank account, the bank should be precluded from disclosing that to the person. Should the RCMP also be precluded from releasing info to the public?

Rogerson: We’re often working on just a tip, or a malicious person.... So, we’d like people who are providing us with info to consult with us before releasing it. It could be life-threatening. The accused could know that someone gave us their name... It’s just the beginning. As law enforcement officers, we start off with the idea that people are innocent. We don’t go to work wanting to put people in jail – we go to work not knowing what to expect. We’re just talking about the first scene here – we don’t even know what the scene is.... It’s very low level information. But it could spur on, within a month, a very violent situation.

Dhaliwal: You’re telling me that you should also be precluding the info getting out. You should also be not disclosing that there’s an investigation going on?

Rogerson: Right.

Wallace: I’m very proud of the RCMP. One thing that’s helpful for us – is there legislation in other jurisdictions with actual wording you’d like to suggest for the bill? Have you actual wording that you’d like to see changed?

McColl: For 7.3.c.i – we would ask that when a police officer, in the course of duty, makes a request, that a company is authorized to give the info.

Wallace: So you believe for the 30% or 40% of ISPs who are reluctant to give the info, that will change with this wording. In terms of the ISPs who are not providing info – does size matter?

McColl: That’s correct – the large ones are most cooperative, some smaller ones are also, but there are 900-1000 ISPs operating, and legal counsel often advises them not to disclose.

Stanton: 7.3(b) – that’s all about disclosure. Not collection, so the information would have to be existing. The only reason under 7.1 that you can collect is when there’s the contravention of a law.

Laforest: I understand there’s some confusion in the public about when to cooperate. You say that it worked well at the beginning, but later you say that art. 7 has problems. I find that contradictory.

Rogerson: There are 30-40% of ISPs who refuse to give us info without authorization.

Laforest: I don't understand why you say that the same section permits you to collect the information, and it's causing you problems – isn't this contradictory?

Crockett: There are people who cooperate well, but there are more and more companies – their counsel who want to advise their clients to be risk adverse. We understand the act to be enabling, but they want to reduce the risk and ask for a warrant. Because it's not clear in all cases, there's a trend to move towards being more risk adverse.

Van Kesteren: Service providers – out of curiosity. Do they not want to give up information because certain providers are known for that?

Crockett: In some cases that's true because they host adult websites etc. We're not going to get 100% compliance, but we'd like to increase our ratio.

Van Kesteren: Aren't there laws in place?

Crockett: Yes, there should be.

Van Kesteren: The current Act has been criticised as not having any teeth. Does the Act allow for the same action by the Commissioner as the police? Should it? Does it give the Privacy Commissioner the power to publicly chastise the police?

Rogerson: Yes. ... She's part of the oversight mechanism.

Van Kesteren: If they're a party to the crime, can the ISPs be charged?

Crockett: Yes, for aiding and abetting.

Martin: I do understand the point you've raised. I'm trying to go beyond that to see what PIPEDA means in, let's say, terrorist investigations. If there's just a suspicion – wouldn't that fall under the rubric of tainted evidence – if the collection violated the person's expectation of privacy? It opens the door because private organizations don't operate the same way as public ones. I think it's a slippery slope.

McColl: If they're acting on the direction of the police, then they're an agent of the state, and there are considerable checks and balances in place.

Martin: That's precisely what's in the Public Safety Act.

Crockett: That is true in any type of investigation. PIPEDA protects the person who has shared that info with the police. But the court still protects the Charter – still holds the police accountable.

Chair: Excuse me – what wording are you referring to, Mr. Stanton?

Stanton: I am getting the sense from the RCMP that they could either ask the private sector to collect information, or the private sector could collect info on their own.

Rogerson: They gather the info, when it gets to us, that gives us the footing to decide whether its investigation time. They could start gathering information for their self-protection. In the old days, we'd have to catch the bank robber outside the door. Now, they could call us...

Martin: PIPEDA is all about protecting people's privacy, we've left a loophole big enough to drive a truck through...

Chair: S. 9 – has certain grounds listed on which you can object to the fact that you're investigating someone. You're not suggesting that those grounds be, somehow, taken out. The grounds for objection should still be there.

Rogerson: Right now, there are a number of groups which....

Chair: You want to be able to object where the provider gives the information, or that they should ask you first?

Rogerson: We don't know at the time if the info is dangerous, but we will if they contact us.

Dhaliwal: If you disclose information, then it can jeopardize information completely. So, the way I look at it is, if this person who was called by the RCMP tells the person who's being investigated...

Rogerson: Going through the white pages is like looking for a needle in a haystack. We are willing to accept the risk, and in the end we'll take it on ourselves.

Dhaliwal: This person goes to the suspected person and tells you that the RCMP is looking for you, that's a disclosure with jeopardizes the investigation. Doesn't disclosing to the collector already jeopardize the investigation?

McColl: We also are governed by privacy rules in investigation, so we seek to disclose as little info as possible in investigation – sometimes we leave an impression anyway, but that's part of the investigation.

Dhaliwal:...

Rogerson: [Describes complaints process against police.]

[Dhaliwal gives a rather complicated hypothetical that the committee and witnesses struggle to understand.]

Vincent: ID theft – does it happen often that you do investigations on this?

Answer: Yes

Vincent: If you call someone and ask for personal information, how can the person on the other end of the line know that they're talking to the police?

Crockett: If we ever get a call to speak about a specific investigation, we've done the background.

Vincent: We'll take an internet survey...

Crockett: If we're getting info, we do it face to face. We would only do it by phone if we already have a rapport with the organization. We're the last line of defence for people's privacy. We would never harm someone intentionally.

Vincent: I know you have integrity, but criminals don't. .. How do they know you're legitimate?

McColl: We encourage people to always be certain who you're speaking to.

Vincent: It's easy, though, to fake a letter or a business card.

McColl: The distinction is important because we're only looking for name and address. It's minimal info that we've always been able to get. If the info is even remotely sensitive, the court governs it.

Martin: Tomorrow we will vote on a new bill which we argue creates an id theft kit – the permanent voters list. Does this raise any concern for you? The date of birth – it's a recipe for id theft.

McColl: We discourage you from using that as a PIN number – it's personal information.

Chair: Can we make this relevant to PIPEDA?

[More discussion re: voter's list.]

Vincent: I'm going to finish my story from before. ID theft is a hot topic lately. When we open the door, we know that criminals are as up-to-date as police – that they know what rights police have, and they could put themselves out as police, and collect information in such a role.

Rogerson: It's not obligatory to give over info if you're not sure of the person before you.

Stanton: Anti-Terrorism act – any thoughts on what Parliament should consider on this?

Chair: How is that relevant to PIPEDA?

End of Meeting