

**BRIEF TO THE STANDING COMMITTEE ON
ACCESS TO INFORMATION, PRIVACY AND
ETHICS RE: *PIPEDA* REVIEW**

CANADIAN RESOURCE CENTRE FOR VICTIMS OF CRIME

The Canadian Resource Centre for Victims of Crime (CRCVC) is a national, non-profit victim advocacy group. We provide direct assistance to victims across the country as well as advocate for more services and rights for victims, and for better protection for victims and the public.

In 2000, the CRCVC sent a discussion paper to all Members of Parliament and Senators entitled “Child Sexual Exploitation and the Internet.” We made 20 recommendations, including that legal requirements be imposed on Internet Service Providers (ISPs) to cooperate with law enforcement, creation of a new offence of luring, raising the age of consent, creation of a national tip-line, etc. We are pleased that several of those recommendations have been acted on, such as the creation of the luring offence, but we remain extremely concerned about these issues.

The problem, not surprisingly, is getting worse, and despite the many successes of Canadian law enforcement, police are only able to scratch the surface. As politicians debate the artistic merits of child pornography, squeamish judges refuse to view evidence before passing sentence on offenders, and privacy advocates create hysteria about “big brother”, our police officers sit in front of computers everyday talking to pedophiles, sorting through the tens of thousands of images of child pornography to catch the predators and stop the abuse of children.

Their objectives are simple – arrest those who create, distribute and access child pornography and identify and rescue those children who have already been harmed. As we see organizations representing the ISPs pat themselves on the back for taking moderate steps to block child pornography sites, the CRCVC would like to acknowledge the men and women in law enforcement who do this difficult work.

SCOPE OF THE PROBLEM

Before addressing our specific concerns about *PIPEDA* and the evidence the Committee has heard to date, we want to explain how serious this problem has become. The Internet has created a whole new playground for pedophiles and child abusers.

In 2005, OPP Detective Inspector Angie Howe told a Senate Committee, “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.”

Internet facilitated child sexual exploitation is a \$2-3 billion industry.¹ There are over 14 million sites that carry child pornography and over 20,000 new child pornography images

¹ Dr. Roberta Sinclair (NCECC) at Canadian Association for Victim Assistance Conference, October 2006.

are posted every week..² In the past, most child pornography was recycled over and over again, but now new material is becoming the norm. That means more victims.

The National cybertip line (www.cybertip.ca) received almost 6000 tips in its first year of operation. There are over one million images of child pornography available on the Internet involving at least 50,000 individual child victims of sexual abuse.³ In Canada, about 50-100 children have been rescued.

While testifying before the Standing Committee on Justice and Human Rights on Bill C-2 in 2005, Dr. Peter Collins referred to an unpublished study that was being conducted by the U.S. Department of Justice in Butner, North Carolina. The researchers examined 54 inmates who participated in a sex offender treatment program. All 54 had been convicted of crimes involving the production, the receipt, and/or the possession of child pornography. Using pre-sentence reports of that group, 46% appeared to have had contact offences. After treatment, and when asked to undergo polygraph examination, 79.6% then admitted that they had contact offences against children--totalling an additional 1,371 victims that had never been detected by the criminal justice system.”⁴

RCMP Supt. Earla-Kim McColl, who runs Canada's National Child Exploitation Coordination Centre (NCECC), says 80 per cent of the images involve some kind of penetration -- oral, anal or vaginal -- and a significant number, about 20 per cent, also involve torture and bondage.⁵ The images are so horrible that in some jurisdictions, Canadian judges won't even look at the photos before passing sentence.⁶

COMMITTEE HEARINGS

The Committee has heard from almost two dozen individuals and groups who have addressed a variety of issues related to *PIPEDA*. Yet not one group or witness has expressed any concern about the privacy violations of the children whose images are being traded like baseball cards every day for the sexual satisfaction of pedophiles and predators. There is no greater violation of privacy then having images and videos of someone raping you distributed around the world. These crimes are facilitated by private companies in Canada who provide broadband Internet access, provide virtual storage areas for abuse images, provide anonymous e-mail, forums for pedophiles to support each other in the belief that having sex with children is good, etc. Companies in Canada are providing the means to allow crimes against children to flourish and they are making substantial sums of money from it and yet the Committee heard no reference to these children and their rights when the Privacy Commissioner testified. We are confused and disappointed that she has not been advocating for these children and their privacy interests.

² “14 million sites carry child porn, says former cop.” Vancouver Sun, October 24, 2006.

³ Ontario Ministry of Attorney General, CAVA conference, October 24, 2006.

⁴ Standing Committee on Justice and Human Rights, Bill C-2, May 3, 2005.

⁵ CTV.ca, July 23, 2006.

⁶ Globe and Mail, October 10, 2006.

Children have been discussed briefly in testimony. There was some reference to their emails being tracked. Another witnesses talked about the issues related to surveying children.

Issues surrounding law enforcement concerns have also received little attention. The witnesses from the Department of Industry told this committee that law enforcement has no complaints about how *PIPEDA* affects their work. This is contrary to the reports that we have read in the media, in which law enforcement investigators have expressed concerns and frustrations that *PIPEDA* impacts on their ability to enforce the laws and protect these children.

PIPEDA

RCMP Sgt. Janis Gray has been quoted as saying, “Our Internet service providers and the credit card companies are not doing what they should be doing – morally and socially.”⁷ Staff Sergeant Mike Frizzell of the RCMP’s National Child Exploitation Coordination Centre has further stated that police are at the mercy of ISPs that can either provide a customer’s name or cite privacy concerns. “That information, for some reason, is kept secretively and only some ISPs will actually recognize its significance and co-operate to keep the community safe – others simply do not. There are a large number that do not and had (the St. Thomas suspect) been with those networks, we’d still be looking for him and that little girl would still be being abused.”⁸

Tom Copeland, head of the Canadian Association of Internet Providers, has stated that ISPs will co-operate in *most* cases if presented with a warrant or letter of authority but “It’s a management decision by each and every ISP, but I think the *trend*, especially when it comes to child exploitation, is to co-operate with law enforcement - subject to some basic lawful authorization.”⁹ Mr. Copeland also said that requiring a search warrant for police to get a suspect’s name and address is “over-kill” and that information is not normally considered private.

The Canadian Coalition Against Internet Child Exploitation (CCAICE)’s 2005 Action Plan, they announced they would “identify how and when Canadian ISPs CAN disclose information to law enforcement...and would promote the implementation of *best practices*.” The Privacy Commissioner says it is her understanding that “organizations deal with these requests on a case-by-case basis.”¹⁰

It is our position that trends to co-operate, promoting best practices and co-operating on a “case-by-case” basis or even in most cases is simply not good enough when it comes to the safety of children.

⁷ “More help needed to fight exploitation,” Vancouver Sun, September 16, 2006.

⁸ “Police probing Internet crimes at mercy of service providers,” St. Catharines Standard, November 8, 2006

⁹ “Police probing Internet crimes at mercy of service providers,” St. Catharines Standard, November 8, 2006

¹⁰ Letter to Canadian Resource Centre for Victims of Crime, December 18, 2006.

It is our understanding that *PIPEDA* is hampering the ability of investigators to conduct investigations and secure subscriber information from ISPs. Mr. Simpson, from the Department of Industry, touched on this, but did not offer any guidance to the Committee or speak to how the legislation might impact child victims of Internet exploitation. He said, “there is an issue around what constitutes lawful authority.”

He was referring to subsection 7(3)(c) of the legislation, which sets out provisions where an organization **may** disclose personal information without consent. The first condition is when it is in compliance with a subpoena, warrant or court order. The second stipulation, which we contend has led to some confusion, is in response to a request by a government institution that has the *lawful authority* to obtain the personal information for the purpose of enforcing a law, carrying out an investigation related to the enforcement of the law, or gathering intelligence for purposes of enforcing a law.¹¹

It is the term *lawful authority* that is at issue. On December 18, 2006, the Privacy Commissioner wrote the *CRCVC* and stated that under section 7(3)(c.1)(ii), “the decision to disclose the information rests with the organization...In other words, the disclosure is discretionary on the part of the organization.” Unfortunately, the view that the information can be disclosed is not shared by all.

In *S.C. (Re)* [2006] O.J. No. 3754, Bell Canada cooperated with Toronto Police in its effort to continue its investigation into a child sexual exploitation suspect. Toronto sent a “Letter of Request for Account Information Pursuant to a Child Sexual Exploitation Investigation” to Bell Canada “under the authority of *PIPEDA*.” The information provided by Bell was then used to try and obtain a warrant to search the suspect’s home. In this case, the court decided that Bell Canada did not have the right to share the information because of the wording in *PIPEDA* and denied the warrant. The court said, “s.7(3)(c.1)(ii) by itself does not establish what “lawful authority” is.”

Fortunately, this decision was overturned and a warrant was issued and the search led to the discovery of a child pornography collection, the production of a controlled substance, and firearms offences.

Committee members may ask why police do not simply get a search warrant whenever they need to obtain personal information. Richard Simpson who testified before this committee said, “In some cases on the Internet, when you’re moving very quickly, law enforcement cannot produce a paper warrant.” But more importantly, in our opinion, police do not and should not need a warrant to secure subscriber information or in any other circumstance except when dictated by Parliament.

¹¹ Section 7(3)(c.1) states that an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is “made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that (i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs, (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or (iii) the disclosure is requested for the purpose of administering any law of Canada or a province;”

Police do not need a warrant to check your license plate in order to identify the owner of a vehicle that is suspected of being involved in a crime. There are many examples like this where the police have access to information that the average citizen doesn't. They have access to this information as they are tasked with preventing and investigating crime and they have an already well established legal obligation not to disclose the information that they obtain except within the course of their mandated duties. Due to *PIPEDA*, it would appear that law enforcement has better access to information about people who fail to yield than they do those who sexually abuse children.

Given the confusion that exists, **we recommend (at the minimum) that section 7(3) be amended to make it clear lawful authority does not mean a warrant.**

We further recommend an amendment, at least in the case of investigations involving child abuse or child pornography, to stipulate that ISPs shall cooperate with law enforcement. The spirit of this amendment was contained in Bill C-74, which was introduced by the former government.¹² It is important to note that other countries, such as the U.S., the U.K. and Australia, already have such laws.¹³

In reference to the companies that do cooperate with the police, ISPs have expressed concerns that, "providing lawful access services to law enforcement agencies, such as providing subscriber information...would generate high ongoing costs in terms of personnel, training and security."¹⁴ In one case in which law enforcement was seeking information to assist in a homicide investigation, Telus argued they should be exempt from complying with the warrant because the financial burden would be unreasonable.¹⁵ The court heard evidence that the **annual** costs to comply with production order requests would be over \$660,000. However, this expenditure was 0.0087% of Telus's operating revenue and 0.12% of their net income for 2004. It was not, to use the words of the forensic auditor who presented the information to the court, "a material amount."

The court went on to discuss the obligations that all citizens have to cooperate with investigations and the justice system. Citizens are required to report for jury duty when called, and we are currently witnessing twelve such citizens who may be sitting in a Vancouver courtroom for an entire year. Citizens may be legally obligated to be witnesses and wait for days to testify, potentially at risk to their own safety. Furthermore,

¹² 17. (1) Every telecommunications service provider shall, in accordance with the regulations, provide to a person designated under subsection (3), on his or her written request, any information in the service provider's possession or control respecting the name and address of any subscriber to any of the service provider's telecommunications services and respecting any other identifiers associated with the subscriber.

¹³ "Telecommunications and Lawful Access: The Legislative Situation in the United States, the United Kingdom and Australia," Dominique Valiquet, Library of Parliament, February 28, 2006.

¹⁴ "Telecommunications and Lawful Access: The Legislative Situation in Canada," Dominique Valiquet, Library of Parliament, February 21, 2006.

¹⁵ *Her Majesty the Queen and Telus-Mobile Company (TELUS) Ontario Court of Justice (2006) File #4911998046559*

the Department of Justice estimates that victims are responsible for almost 70% of the costs of crime.

We further recommend an amendment to make it clear that *PIPEDA* was not meant to negate or interfere with the moral and ethical duties of companies to be good corporate citizens and assist the police, as any good citizen would, in preventing and investigating crime. This could be accomplished by strengthening section 3 to include protection of the privacy of child victims of Internet exploitation and emphasize that personal information should be actively disclosed in investigations aimed at protecting children.

Finally, we would ask the committee use its influence to express to the Office of the Privacy Commissioner a desire to see her office become an advocate for the child victims of Internet sexual exploitation who face unique privacy challenges that, in addition to the torture they suffered, add an additional level of abuse. The Office of the Privacy Commissioner could, for example, begin to examine what steps ISPs can and should be taking to prevent their services being used to distribute and store child sexual abuse images and to remove images once they are identified. Last year, her office gave several grants to various groups to conduct research, among them issues affecting privacy policies aimed at children. There was no mention of child victims of Internet sexual exploitation and their needs, nor did she advocate for ISPs to recognize and honour the privacy rights of child victims.

We will end our brief with the words of a young woman who was repeatedly sexually abused. Her abuser took photos of her and posted them on the Internet. Her victim impact statement has been used in courts involving the sentencing hearing of a man who had photos of her. With all due respect to the other witnesses and the serious issues they raised, if you remember only one voice during these hearing, let it be this excerpt from her statement:

“I can't even remember all the abusive things he did to me. Unfortunately, though, I can't forget because there are pictures of the abuse. Hundreds and hundreds of pictures of (him) doing horrible things to me ...

The absolute worst thing about everything that happened to me was that (he) put my pictures on the Internet. He traded them with other people like baseball cards. What kind of people want to see pictures of a little girl being abused in this way?

I have been told that my pictures are the most popular on the Internet. How can so many people delight in the horrible things that happened to me?

I still don't really understand why this happened to me or why so many people want to see these terrible things. I know that these pictures will never end and that my "virtual abuse" will go on forever. Usually when someone is raped and abused, the criminal goes to prison and the abuse ends. But since (he) put these pictures on the Internet, my abuse is still going on.

Anyone can see them. People ask for them and are still downloading them. Day after day. People want to see me being abused. I want every single person who downloads my picture to go to jail and really be punished as much as possible. They are as evil as (him). They want to see me suffer. They want to see me starved and hurt and sad and abused.

Child pornography is not a victimless crime. I am a victim and I still suffer everyday and every time someone sees me being abused. I ask that you think about me and everything I have gone through....”