CUSTOMER NAME AND ADDRESS CONSULTATIONS

Public Safety Canada

By: Canadian Resource Centre for Victims of Crime

October 10, 2007

Introduction

The Canadian Resource Centre for Victims of Crime (CRCVC) is a non-government, non-profit advocacy group for victims and survivors of violent crime. We provide direct assistance to victims across the country as well as advocate for more services and protections for victims and the public. We were pleased to receive an invitation from Public Safety Canada to participate in the consultation process regarding possible measures to address law enforcement and national security agencies' lawful access to customer name and address (CNA) information held by telecommunications service providers (TSPs).

As a non-government organization dedicated to ensuring the voice of victims and survivors is heard, we agree that the rights and freedoms guaranteed in the *Canadian Charter of Rights and Freedoms* must be protected. However, the protection of an individual's privacy cannot take precedence over the protection of the public from national security threats or the protection of children from sexual exploitation.

Canada is in no way immune to terrorist threats, as seen with the arrest of a Quebec man in connection with an online plot to bomb targets outside Canada on September 14, 2007. If not for the prompt response of the RCMP and other law enforcement groups, a serious incident may have occurred.

We have long advocated for increased protections for child victims; including those who may be sold, prostituted or used for child pornography. Our largest area of focus has been on advocating for increased resources for law enforcement to allow them to fully investigate and rescue children from sexual exploitation on the Internet.

As stated in the consultation document, law enforcement has repeatedly voiced their concerns about the difficulty in consistently obtaining basic CNA information in the course of their duties. Officials need prompt cooperation from TSPs in order to prevent threats to national security/public safety and to rescue abused children. It is our opinion that corporations should be obligated to assist law enforcement (without a warrant), as any good citizen would, in preventing and investigating crime.

Our position

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, the creation of a new offence of luring, raising the age of consent, creation of a national tip-line, etc. It is unfortunate that seven years later, law enforcement agencies still face challenges accessing basic CNA information.

The lack of explicit legislation in this area gives telecommunications companies the discretion to provide information to law enforcement when it is requested or to demand a court order before releasing any information at all, regardless of the situation at hand. This is problematic at any stage of an investigation, likely halting it or creating significant delays while documents to compel the information are sought. We should not have to reiterate the risk of delays in the context of preventing terrorism or rescuing children from sexual abuse. We believe the government should immediately amend section 7(3) of the *Personal Information Protection and Electronic Documents Act (PIPEDA)* to make it clear that 'lawful authority' does not require a warrant in order to ensure the police and national security agencies are granted CNA information.

We fully support the use of safeguards, as listed in the consultation document. In order to prevent abuses, for example, we support limits on who can have access to the information, limiting how it is used, and internal audits on the use of the powers, etc. We agree that lawful access to CNA information should not include the content of communications or the web sites an individual visited online unless a court order is issued.

Concerns of privacy advocates

The problem of child pornography on the Internet is getting worse, and despite the many successes of Canadian law enforcement, police are only able to scratch the surface. We applaud the continued, difficult work of police officers in sorting through tens of thousands of images of child pornography in order 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.

Some privacy advocates suggest, "Canadian law enforcement and national security agencies are looking for a quick and easy way to obtain access to the names, phone numbers, IP addresses,

etc…of customers of Canadian telecommunications service providers. Quick and easy, in this context, means without the delay and paperwork involved in applying to a judge for a search warrant."[1] We urge officials to remember that police/national security officials seek this information in a number of contexts, including in the very beginning of investigations or as part of intelligence gathering. We submit that persons who come to the attention of law enforcement or national security agencies in the course of their investigative duties are 'persons of interest'. Their actions online have raised serious red flags. We do not believe that CNA information is sought when there is insufficient evidence to connect an individual to a crime so that a judge would not issue a warrant, or so officials can go searching for crimes that may be occurring outside of the scope of their investigation.

Law enforcement and national security agencies must act quickly when such 'persons of interest' come to their attention. There is not always ample time to obtain lawful authority in the form of a warrant. Immediate threats to national security and the sexual abuse of children must override the protection of anyone's personal information by *PIPEDA*.

We urge Public Safety officials to remember the privacy violations of the innocent 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. We cannot allow these crimes to continue to be facilitated by private companies in Canada who provide broadband Internet access, virtual storage areas for abuse images and anonymous e-mail, and forums for pedophiles to support each other in the belief that having sex with children is not wrong.

Tom Copeland, head of the Canadian Association of Internet Providers, has stated that requiring a search warrant for police to get a suspect's name and address is "over-kill" and that that information is not normally considered private. We agree, and would submit, that much of the "personal information" held by TSPs is already public information contained in most telephone directories.

We also submit that cooperation by TSPs on a case-by-case basis, which is what generally occurs now, is simply not good enough when it comes to the safety/protection of children or threats to

[1] David T.S. Fraser, "Some necessary background information to the fuss over warrant-less access to Canadian personal information," 15 September 2007. http://www.privacylawyer.ca/blog/2007/09/some-necessary-background-to-fuss-over.html

national security. Privacy advocates maintain that there must be court oversight in order to hand over personal information and that police investigations have not been hampered to date. However, investigations have been hampered, as reported by many police officers during the Statutory Review of *PIPEDA* in 2006/2007. 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.

Police do not need a warrant to check a license plate in order to identify the owner of a vehicle that is suspected of being involved in a crime. There are many examples where law enforcement has access to information that the average citizen does not. They have access to this information because 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.

The Problem

As *PIPEDA* currently exists, it requires the consent of the individual for all collection, use and disclosure of personal information, subject to a number of exceptions. "Personal information" includes any information about an identifiable individual. It is thus illegal for TSPs to disclose such information without consent.

What constitutes *lawful authority* is at question. Subsection 7(3)(c) of the legislation is where the confusion occurs, as it 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 for disclosure 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.[2] The second condition should be treated independently of the first, yet in our meetings with law enforcement we have heard that TSPs tend to treat these two conditions as one. Thus, they are interpreting *lawful authority* to mean a warrant is always required.

[2] 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;"

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." We submit, once again, that discretionary disclosure is simply unacceptable when it comes to public safety and the sexual exploitation of children.

CRCVC Recommendations

Given the confusion that exists regarding lawful authority and the hesitation of some TSPs to comply with law enforcement requests, we recommend (at the minimum) that section 7(3) be amended to make it clear 'lawful authority' does not mean a warrant is required. Lawful access to CNA information at the outset or during the course of an investigation should be clearly defined.

We further recommend an amendment, in the case of investigations involving child abuse/child pornography and threats to national security, to stipulate that TSPs shall cooperate with law enforcement.

Thank you for the opportunity to participate.

Respectfully submitted,

Heidi Illingworth
Executive Director