CUSTOMER NAME AND ADDRESS INFORMATION CONSULTATION

NCECC – RCMP SUBMISSION TO PUBLIC SAFETY CANADA

October 2007

INTRODUCTORY REMARKS

The National Child Exploitation Coordination Centre (NCECC) of the Royal Canadian Mounted Police (RCMP) welcomes the opportunity for broader public consultation on "issues associated with the question of accessing customer name and address in the modern telecommunications world."[1] NCECC would like to state at the outset that a legislative solution is becoming essential. It is needed to require or compel telecommunications companies to provide basic customer identifying information to police upon receiving a formal request. Without a statutory requirement imposed on them, these companies can choose (under the common law) to do nothing. Even though police have a longstanding authority under the common law to ask people questions in the lawful execution of their duties, there is nothing presently in legislation to require these companies to respond positively.[2] As long as they are at liberty to decline to provide this information to police upon request, investigations can and are being impaired. In the case of online child exploitation matters, the result is that many investigations actually cannot proceed. Misunderstandings surrounding the common law authority of police to seek this information without having to first obtain a court order have already had serious consequences for child exploitation investigations and victims.

Since the establishment of NCECC in 2004, the single most important challenge facing investigators of Internet facilitated child exploitation, ahead of all other issues, has been their inability to obtain basic customer information, such as someone's name and address, from Internet Service Providers (ISPs). However, it is important to note that NCECC operations are not the only operations that are seriously affected. The "CNA problem," as police tend to call it, has been on law enforcement's radar screen, becoming an increasing impediment to effective police operations, since early 2000.[3]

---

[1] "Customer Name and Address Information Consultation" document posted at http://publicsafety.gc.ca.

[2] See *R.* v. *Turcotte*, [2005] 2 S.C.R. 519 at para 41 where the Supreme Court of Canada (SCC) noted: "Under the traditional common law rules, absent statutory compulsion, everyone has the right to be silent in the face of police questioning.

[3] Canadian Association of Chiefs of Police, "Response to Government of Canada's Lawful Access Consultation Document", 16 December 2002, http://www.cacp.ca. The CACP, in 2002, noted at p. 1-2:

> [W]hile communications technology has continued to rapidly advance, the ability of police to retain access capabilities and gather the necessary information to detect and apprehend criminals has not. This gap in the relationship between law and the reality of today's technology now poses a significant threat to public safety and the attenuation of police effectiveness. It is creating a safe zone where serious criminals, such as organized crime and cyber predators, can operate free from fear of detection and apprehension. … Internet Service Providers have been very reluctant to

The NCECC finds that the Internet has created an environment where sexual offenders can operate with increased anonymity, while police operate with increased difficulty accessing their basic identifying information. The NCECC attributes this growing phenomenon to the misconception that a customer's name and address, when the customer is online, is more private and should have more protection from reasonable police access than the name and address of a telephone customer that appears in a telephone book.

In this submission, the NCECC will be discussing the CNA issue mainly in the context of investigating Internet facilitated child exploitation. However, the impediments that NCECC investigators as well as other police officers encounter routinely in trying to identify offenders on the Internet, are not unique to investigative operations. Police face challenges obtaining CNA in all their mandated work, that is, from general (non-investigative) policing duties to investigations of the most serious criminal offences. Consequently, many of the observations that the NCECC will be making in this submission apply to all aspects of RCMP operations, and indeed to the work of all police agencies in Canada.

Police understand, value, and respect the importance of protecting individual privacy. We also understand that privacy interests must be balanced with other public interests, for example, the public interest in keeping members of our communities safe, in preventing injuries and crime, and in successfully charging criminals for their offences. In our experience the success of policing operations in our communities depends on ensuring that a reasonable balancing of these interests is achieved.

The NCECC understands that the legislative proposals, which have been under consideration for the past few years, were designed to create an administrative framework to govern requests for customer information. That framework would include clear legal rules both for police to obtain and for telecommunications companies to release basic customer identifying information, such as a customer's name and address.

Much of the public debate surrounding police access to customer name and address information, so far, has concentrated only on one issue – whether police should, or should not, be required to obtain the prior authorization of a court in order to lawfully access this information. The NCECC will address that important question in this submission. In addition, this submission will attempt to explain why the RCMP, including the NCECC, has reached the conclusion that legislative support is necessary, and why in the RCMP's view the proposed administrative model --rather than criminal legislation creating a new warrant or court order -- is the logical choice for police to obtain this information.

The remainder of this submission consists of two parts. The first part outlines the challenges and issues that arise for the NCECC (and the RCMP generally) in seeking to identify users of Internet services. The second part discusses law enforcement's

---

provide information about registered users even when these clients are engaged in dangerous criminal behaviour.

preferred solution: legislation adopting an administrative model to govern how police and telecommunications companies handle requests for information identifying their customers.

PART ONE:
CHALLENGES & ISSUES FROM A POLICING PERSPECTIVE

The Internet has revolutionized our lives in a tremendously positive way but it also poses significant risks to adults and children. For adults the risks are mostly economic; however, for children the risks are to their personal safety and security.

Historically, Canadian law has been predicated on the belief that community safety was a mutual goal and for that reason, until very recent times, there have been few laws needed to compel the cooperation of certain sectors. Unfortunately, in the online world, the sense of a civic duty or public responsibility to assist police, for example with identifying customers, appears to be diminished. The state can no longer count on the voluntary cooperation of certain corporate citizens in the online world to ensure community safety.

In the past telephone companies were the traditional source of customer name and address information for police. They voluntarily assisted by providing basic name and address information to identify customers using their services. Today certain companies as well as Internet Service Providers (ISPs) resist and regularly refuse to assist in this way. For these companies this change may be due in part to legal obligations they have had since 2000 to protect the privacy of their customers' personal information, confusion over the "lawful authority" of police to request this type of non-sensitive customer information without first obtaining a warrant, and their desire to avoid potential litigation and corporate liability for alleged privacy violations. As a result, police now find themselves asking federal lawmakers to contemplate enacting laws compelling these companies to provide this basic customer identifying information to police.

The NCECC notes that some critics have opposed these proposals because they consider such new laws to be an unjustified extension or increase in police powers. However, it is the view of the RCMP, including the NCECC, that these proposals would not provide police with "new" powers. Rather they would be legislative provisions confirming an established authority police have under the common law. The proposed legislation, in effect, would compel telecommunications companies to cooperate in situations where certain companies now exercise their right under the common law to say nothing. As a result, the legislation would affirm the existing authority of police to ask, while clarifying for companies that they must provide this particular information on request.

Federal lawmakers have been asked by the CACP and other policing organizations to resolve the "CNA problem" in order to preserve the ability of police to continue to obtain non-sensitive customer information upon request (and without a warrant). From an operational perspective, this proposed legislation would enable police to regain lost

ground in terms of being able to readily acquire non-sensitive customer information that is critical to the effectiveness of daily police operations.

In the remainder of this Part, the NCECC will be discussing the following considerations, which we believe to be important in assessing how to resolve the challenges that police are facing in obtaining CNA and other basic customer identifying information:

1. Problems with the status quo;
2. Police are not requesting personal information that is confidential or sensitive;
3. Warrants may not be feasible or possible to obtain this basic information;
4. Unnecessary demands for warrants place an added burden on the Justice system;
5. Time delays, resource impacts, consequences for victims;
6. Public expectations of police;
7. ISP obligations;
8. Statistics supporting the need for legislative response; and
9. Public support for police efforts.

1. Problems with the status quo

The NCECC would like to note that the level of cooperation by Canadian ISPs ranges from excellent to non-existent. Many of the large Canadian ISPs in this country are willing to assist and usually meet, and occasionally exceed, our expectations when called upon for assistance. Our success in rescuing children and investigating offenders who pose a risk to children, is a direct result of their cooperation. However this is not universal amongst all ISPs. Our statistics of thwarted investigations at the NCECC averages 33%. One third of all requests, per month are refused, not responded to, or we are advised that the data is no longer available. A few small ISPs openly advertise their lack of cooperation with police to attract customers.

The cooperation NCECC does enjoy is the result of more than two years of negotiation and legal analysis by ISPs' legal counsel who form part of the Canadian Coalition Against Internet Child Exploitation (CCAICE). This coalition is comprised of ISPs, government representatives, Cybertip and interest groups. Together we have developed an administrative process very similar to proposals made to address the CNA issue with an administrative framework set out in legislation. The difference is that the CCAICE model is voluntary and ISPs are not required by legislation to do anything to assist police. As a result, numerous impediments and many outstanding issues arise with the CCAICE model. They include:

I. **Inconsistent Cooperation:** Since participation of ISPs is completely voluntary, they may withdraw at any time. There are apparently over 400 Canadian ISPs. Many are not participating fully and consistently.

II. **Refusal to Cooperate**: Some ISPs constantly refuse to cooperate. Currently five ISPs are known to do so. Furthermore, after police approach them for assistance to identify the individual associated with an IP or email address, there is nothing prohibiting the ISP from informing their customer about the police inquiry.

III. **Delays:** There are no obligatory time frames for assisting police. For example, in one case while investigating real-time on-line sexual assaults the investigator requested CNA in an effort to locate and rescue the children. The ISP advised the investigator to call back after the weekend and during business hours.

IV. **Unenforced Customer Agreements:** ISP customer agreements indicate that ISPs will cooperate with police if the customer is using the service to break the law. However, these agreements are between the service provider and their customers. They do not create any legal obligation for ISPs to assist police by helping to identify persons committing offences online. That type of assistance is voluntary.

V. **Unreported Criminal Behaviour:** Although most ISP customer agreements prohibit unlawful activities and stipulate that they will report criminal acts, NCECC was able to locate only one instance where a Canadian ISP had discovered suspected child pornography and reported it to the RCMP.

VI. **Investigative Limitations:** Participating ISPs will only voluntarily provide CNA in Internet facilitated child sexual abuse cases. Requests for CNA related to other criminal investigations and public safety threats are normally refused. So, if police are alerted to a person who has posted threatening material on the Internet and who may pose a serious risk to public safety, currently they cannot count on the assistance of that person's ISP to identify him. In the aftermath of a recent school shooting, it was discovered that the shooter had posted disturbing material on the Internet. This incident highlights potential dangers that might be averted if police were actually able to obtain CNA when public safety could be at risk.[4]

VII. **Inadequate Retention Periods:** ISPs are not required to retain customer data, such as IP addresses used by a customer, for any fixed period of time. This can negatively impact many investigations. In some instances, data is purged after four hours. So by the time police request certain information, it no longer exists.

VIII. **Inaccurate Information:** Some ISP's stipulate that they cannot or will not ensure the accuracy of the CNA information provided.

---

[4] See e.g.,
http://www.cyberpresse.ca/article/20060914/CPACTUALITES/60914017/6096/CPACTUALITES. Here it was reported:

> On peut également voir dans des quotidiens des photos du suspect sur un site web. Kimveer Gill y exhibe fièrement plusieurs armes. Il y a pratiquement laissé sa biographie dans laquelle le jeune homme se décrivait comme un solitaire qui ne s'entendait pas avec ses parents, qu'il était très tourmenté et détestait les sportifs et la société en général. Il a notamment écrit qu'il souhaitait mourir soit «comme Roméo et Juliette ou sous une pluie de balles.»

IX. **Email Addresses Versus IP Addresses:** Many ISPs are unwilling to provide the NCECC with CNA from an email address rather than an IP address. NCECC is unable to explain why ISPs make this distinction.

In an effort to gain further cooperation there have been numerous meetings, telephone conferences, consultations with corporate legal counsel, the support and intervention of proactive ISP counsel and counsel from the Ontario Attorney Generals office. However, despite these ongoing efforts, the NCECC has failed to sway some companies.

The CCAICE administrative model was a welcome initiative and in NCECC's view one of the most significant undertakings, to date, by the Canadian Coalition Against Internet Child Exploitation. Nevertheless, in light of these shortcomings, NCECC, the RCMP and other police forces now find themselves asking federal lawmakers to contemplate enacting laws compelling these companies to provide basic customer identifying information to us.

2. Police are not requesting personal information that is confidential or sensitive

Judicial authorizations, such as warrants, are designed to protect people's reasonable expectation of privacy. A judge's order is necessary to protect the sanctity of places where an individual has this expectation (for example, home, office) or information that attracts this expectation (for example, an individual's core biographical information such as DNA, medical records, chat logs, and web-surfing history).

While a warrant is required to obtain an individual's core or sensitive biographical information, warrants are not required to access non-core or non-sensitive biographical information. A person's name, address, and phone number, is personal information that is not sensitive -- it is *not* core biographical information about the person. This information does not reveal intimate details about an individual's lifestyle and personal choices. So when police request this information they are not seeking information that is confidential or core biographical information. This type of information is made widely available through numerous avenues, such as call display, phone books and reverse phone number look-up on the Internet.

The public debate surrounding police access to customer information upon request seems to pit privacy interests against the state's interest in protecting the public and investigating crime. The prevailing premise seems to be that the two interests are mutually exclusive. However, it is the RCMP's view that these interests must co-exist and the best interests of Canadians are met by balancing both interests rather than by one winning out over the other. The Supreme Court of Canada articulated that important balance very well by stating "The community wants privacy but it also insists on protection. Safety, security and the suppression of crime are legitimate countervailing concerns." (*R.* v. *Tessling*, [2004] S.C.J. No. 63 at para. 17).

Furthermore in *Tessling*, the Court pointed out that "not every form of examination conducted by the government will constitute a search for constitutional purposes." In *R.* v. *Plant* the Court also clearly established that not all information an individual may wish to keep confidential necessarily enjoys s. 8 protection. (*R.* v. *Plant*, [1993] S.C.R. 281 at 293).

3. Warrants may not be feasible or possible to obtain this basic information

The BC Court of Appeal recently dealt specifically with the issue whether a police request to obtain the name and address of a customer related to certain bank account numbers, so that police could prepare an ITO (information to obtain a warrant), violated the accused's reasonable expectation of privacy. The Court found: "Section 8 of the *Charter* provides that everyone has the right to be secure against unreasonable search. In the case at bar I am of the opinion that there was no search, much less any unreasonable search as envisioned in the *Charter*." (*R.* v. *Quinn*, [2006] B.C.J. No. 1170 at para. 93).

A police request for a customer's name and address related to an Internet account indicates only who is financially responsible for the account. Further investigative steps must be taken to determine who accessed the computer and who may be responsible for the crime. A warrant for the residence or computer would be obtained only once police gather sufficient information to form reasonable and probable grounds as to who may be culpable and determine where evidence is likely to be found.

In the case of Internet facilitated child sexual exploitation offences in Canada, the investigation normally begins when a seizure of evidence from one offender reveals Internet Protocol (IP) addresses of other offenders who have uploaded, downloaded, and/or shared child pornography. When computers "speak" to each other, the IP address is automatically captured along with the date and time of communication. Police then commence a new and separate investigation to identify those responsible.

For example, a recent child pornography case from Germany identified 28 countries and within Canada over 200 IP addresses. Upon receipt, the NCECC attempted to identify the account holders. But some IPS refused to cooperate. In this case, and other examples like it, the investigation begins with, and often ends without, police finding out the name and address of an account holder who was using an IP address assigned by a service provider on the day and time in question.

Police must ask the ISP for the customer name and address associated to each IP address – the ISP is the only one who has that information. At the time of the request, police are at the preliminary stages of an investigation, operating on unsubstantiated information (suspicion) in an investigative process that may or may not establish reasonable grounds. This stage of information gathering is sometimes referred to as the "pre-warrant stage" of an investigation. A warrant cannot be obtained in the investigation of a criminal offence until sufficient information to support reasonable and probable grounds for that offence exists.

Police regularly receive complaints from the public regarding postings where, among other things, people harass others, threaten suicide or display aggressive behaviour. These matters require follow-up to determine if there is an offence and/or if someone is in danger or in need of assistance. This is a critical public safety responsibility assigned to police both on and off line. Unfortunately situations, which begin as these types of complaints, can turn into cases such as criminal harassment, hate crimes, and uttering threats over the Internet and some have the potential to result in injury or death.

In the early stages of police handling this type of matter, police need to identify and / or locate the person involved. The first step in that process is to try to obtain from the ISP the necessary information to identify the Internet customer. If the ISP will not assist police with that first step then their first step often becomes their last step. The ISP is the only one who holds the customer information in question. Police would not have sufficient grounds to form the reasonable belief an offence has been committed, which is required to obtain a warrant or court order, so the police's capability to inquire into the matter would cease with the ISP's refusal to cooperate.

Unlike vehicle license plates, there is no central database for the police to query to identify the individual registered to an ISP's system as the source of a particular IP or e-mail address. Only ISPs have this information and, when they are contacted to provide that information, a number of them routinely refuse such requests.

Other industries readily assist police in identifying persons of interest in the early stages of investigations of offences that occur without the involvement of the Internet; however, when the crime involves the Internet police routinely are faced with having to convince an ISP of their lawful authority to request this information. Without a specific provision in the law to point to as their statutory authority to obtain this information upon request, police are faced with quoting Charter jurisprudence to company personnel and explaining their general statutory powers and common law authorities to them.

Several police responsibilities do not involve criminal investigations but instead involve assisting the public. They are referred to as general policing duties and while they form part of police officers' core responsibilities, they do not involve the investigation of crimes or other offences. However, they also can involve police in seeking to identify the names and addresses of certain people.

These duties, for example, include but are not limited to: notification of next of kin; investigation of reports of "overdue" (not yet officially missing) spouses, hunters and hikers; search and rescue for missing persons; assistance to individuals apprehended under mental health legislation; and assistance to a Coroner in the identification of deceased persons.

A report to police by parents of an "overdue" child is a general policing duties scenario that illustrates a situation where an officer may need to turn to an ISP for assistance in identifying a customer's name and address. When the report (phone call from the parents) is received, the child is not yet confirmed to be missing and police do not have

grounds to believe there has been foul play. Therefore, the facts of the case have not ripened into a criminal investigation. The parents could simply report, for example, that their 11 year old daughter did not return home at the pre-arranged time from playing at the park down the street and they suspect she might have gone to meet her online friend: Johnnie4@small_ISP.ca. When they call police for assistance in locating their daughter, an officer would try to follow-up on their "meeting" tip by seeking the assistance of the parent's ISP in identifying the source (customer name and address) of the Johnnie4 email address. The officer would be trying to gather some basic identifying information related to the source to use in figuring out who he might be -- he might just be a friend in their daughter's class or he could be a convicted sex offender. The ISP customer name and address information would not, of course, tell the police whether Johnnie4 is a friend or a dangerous adult. It would simply lead police closer to making that assessment. However, if small_ISP won't voluntarily give police the name and street address associated with the email address of Johnnie4, then the ability of police to follow-up on the parents' initial lead would be thwarted. This scenario does not involve an investigation, at this stage, where a warrant would even be possible. At this point, a child is overdue and may be missing but police do not have any grounds to believe, or even suspect, an offence has been committed. It is however an important police matter where time is of the essence and where the parents', the police's and the public's expectations are high for police to be able to assist in locating the child and to act quickly.

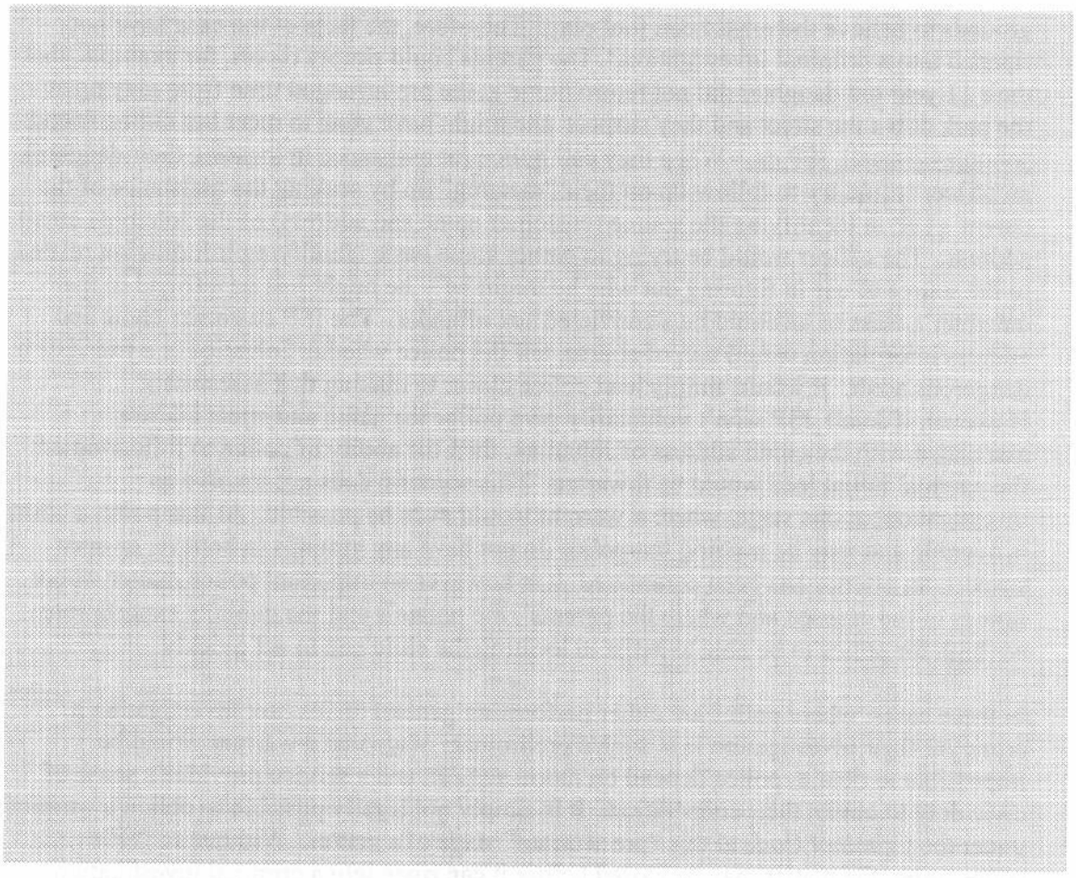
In these cases, where police are either performing general duties (not investigating a crime) or their investigation is at such a preliminary stage that a warrant would be impossible to obtain, police depend on moral suasion and a service provider's sense of civic duty to obtain their cooperation. It is simply not legally possible to obtain a warrant under the *Criminal Code* at this "pre-warrant" stage of a matter. Without an ISP's cooperation, the matter may be closed before it can ripen into a criminal investigation. This type of result is unsatisfactory to police, as well as complainants and the public. In missing children and child exploitation cases, NCECC is concerned that this type of result is particularly unacceptable for the children who are the victims and need to be rescued.

In addition to the situations described above, where obtaining a warrant or court order is **not possible**, sometimes (where it would be possible to obtain the order) it is **not feasible**. In these situations obtaining a court order, such as a production order under s. 487.012 of the *Criminal Code* for an ISP customer's name and address, would be possible because police have reasonable grounds to believe an offence is being committed. However, in these particular cases the customer name and address information, to be useful, is required immediately.

s.16(1)(a)i)
s.16(1)(b)

[redacted]

s.16(1)(a)i)
s.16(1)(b)



4. **Unnecessary demands for warrants place an added burden on the Justice system**

In addition to situations where timing and an immediate need to obtain CNA defeats the purpose of obtaining a warrant, the NCECC and other RCMP investigators have encountered situations where they find service providers are forcing them into obtaining a warrant or order from a court, even though one is not required under the law. In these cases, RCMP needs information to identify a customer but the information in question does not attract a reasonable expectation of privacy and so the prior approval of a court is not required by law. Nevertheless, the service provider -- who is the custodian of the customer information -- refuses to provide it unless police produce a court order or warrant for the information.

For example, law enforcement officers investigating child sexual exploitation offences are often forced into preparing warrants to obtain a customer's "personal information" in circumstances where authorizations are not required by law. They do so to appease liability concerns of certain ISPs who want the clear protection that a warrant can offer against potential liability if an ISP is later accused of disclosing a customer's personal information contrary to the *Personal Information Protection and Electronic Documents*

Act (PIPEDA).[5] Faced with a choice between being able to save a child enduring grievous sexual abuse or unnecessarily using police and court resources to obtain a warrant to satisfy an ISP's concerns, police in some regions have determined that they have no option but to capitulate.

Police in New Brunswick recently completed an extensive investigation and arrested seven suspects on the same day. While the arrests and charges are indicative of the quality of the investigation, it required double the work as uncooperative ISPs demanded warrants before they would produce CNA information for police. Seven search warrants were drafted to compel the ISPs' cooperation rather than because they were required under the law in order to protect a reasonable expectation of privacy. Thus, a total of 14 warrants were obtained in that case, doubling this work for police and the courts.

When compared to other telecommunications service providers, such as the major telephone companies, as well as other industries, certain ISPs are unique among them in terms of the frequency with which they demand warrants for this type of basic customer information before assisting an investigation. Many other companies willingly assist police in similar circumstances to further their work in the prevention, detection, and early stages of investigation of crimes.

It should be noted that other industries, in particular, provide information willingly to police without demanding warrants or questioning the definition of "lawful authority". For example, in a Canadian homicide investigation, the victim's body parts were found in various companies' shopping bags and investigators had already identified an area of the city where the suspect was believed to be residing. So, they contacted these companies and asked for a list of the names and addresses of any customers who lived in this area. If any particular individual then surfaced on several customer lists, he would have been of increased interest to the homicide investigators as a potential suspect. While the killer was ultimately identified via other means, this call for company assistance occurred at a pre-warrant and early stage of investigation. In the end their voluntary cooperation may, or may not, have provided the only clue possible to crack the case. But the point is that these companies did not hesitate when they were asked to volunteer non-sensitive customer information for the purposes of a murder investigation. Their actions demonstrate how good corporate citizenship can facilitate investigations and that other sectors do not demand warrants for non-sensitive customer information.

Historically, telephone companies voluntarily assisted police; however, police now find that these telecommunications service providers, in particular some cellular telephone service providers, are also increasingly reluctant to cooperate.

For example, recently a RCMP police officer had his cell phone stolen. His service provider required him to give written permission to local police so that they could access his telephone records during their investigation. In spite of having the customer's permission, the telephone company refused to provide information about calls made on the customer's stolen phone after the theft. The victim/customer/police officer contacted

[5] S.C. 2000, c. 5, ss. 11 to 17.

the company to enquire why. The company explained its position – it was concerned about protecting the privacy interests (the calling records) of the alleged thief.

Companies do tell police, when they demand a warrant, that they are concerned about being held liable under privacy laws. For those who are concerned about liability and what they perceive to be the legal risks associated with assisting police, normally the only exception they will make is in life and death situations (and even in these situations a few have still refused to provide the non-sensitive customer information they have been requested to provide to police). This is despite the fact that ISPs usually state in their terms of service for customers that if the service is used to break the law they may notify the police. In cases of Internet facilitated child sexual exploitation offences there is no definitive way to assess level of risk to the child until an investigation is undertaken.

If police acquiesce to continued ISP demands for warrants in situations where none are required under the law then their actions will no doubt result in other sectors making requests for warrants prior to cooperating with the police. In cases where an ISP's customer is committing an offence, for example an offence related to child pornography, using the ISP network, at the very least the ISP is a witness.

When investigating known cases of online child exploitation, NCECC members always request customer identifying information from the ISP who holds the IP address and customer identifying information in question. They do so even when the ISP is known to always refuse to voluntarily provide that information to them for the sake of each child/victim who may be a child in need of rescue.

The RCMP, including the NCECC, supports legislative action that would clarify the responsibilities that ISPs have to provide basic customer identifying information to police upon request. Clarifying this obligation in a statute would likely alleviate their concerns over potential liability for disclosing personal information, without an individual's permission and without a court order to authorize the disclosure

5. Time delays, resource impacts, consequences for victims

The NCECC alone makes approximately 200 requests to ISPs per month for customer name and address information. (Data reflecting the level of cooperation from ISPs is documented in more detail below.)[6] All Internet child exploitation (ICE) units make these requests. As already indicated, in many cases obtaining a warrant is not possible or not feasible. Even when it would be possible, the time to complete a warrant, locate and drive to a Justice of the Peace (who is often not in close proximity to the police), wait for the approval, and repeat this process each time another customer's name and address information is needed would place an immense burden on police and court resources across Canada. More importantly, in terms of the potential impact on police, would be the shift in the focus of resources. Finite police resources, previously dedicated to identifying and locating child victims, would now be severely impacted as investigators'

[6] See section 8 of this part of the Submission, titled "Statistics supporting the need for legislative response".

already heavy workloads would begin to involve a heavy concentration of time spent on preparing warrant applications and obtaining a court official's approval for their request. In addition, while this shift in utilization of resources would occur, investigators would be cognizant that the abuse of child victims is ongoing. Information they used to reach for in a phone book, or obtain online through a "Canada411" reverse phone number search, or obtain from simply asking a person, is now denied to investigators not because the customer name and address sought is any different, simply because it is deemed to be somehow different.

Recently an online investigator was approached in a public chat room by an unknown person and advised by that person, that he was about to rape his 12 year old step-daughter and broadcast it live. Obviously, in this situation, police did not know where the offender was physically located but instantly were challenged with preventing the assault. To track the suspect's virtual location (indicated by his IP address, the date and time he is online) into a street location, and to try to catch the suspect before he committed the assault, investigators needed to quickly obtain physical address information from the ISP. Without prompt cooperation, not only could the assault occur but the opportunity to ever trace the offender could be forever lost. While police in this situation in Canada would have the grounds to obtain a warrant for the subscriber's address from the ISP, the law does not require police to obtain a warrant for this type of non-sensitive customer information. Furthermore, by the time a warrant could be drafted, taken to a JP and signed the opportunity to locate and rescue the victim could be lost, forever. In this particular case, the offender's IP address belonged to an ISP in the UK. So the investigation was handed off to UK investigators who were able to immediately obtain the customer name and address information that was needed to locate the offender and to rescue his victim.

6. Public expectations of police

The public expects the police to investigate crimes and keep citizens safe. With the exception of the Internet, in every other domain where there is a potential for crime or harm, there exists a capacity for police to rapidly investigate alleged offences. The NCECC believes that the public would support appropriate legislative action to resolve this problem immediately and to ensure that all ISPs are clear about what customer information they may and should provide to police upon request.

Without customer name and address information, an investigation often cannot even begin into child pornography found online and the evidence it points to of the abuse of a child by a potential sex offender. Several studies indicate that between 30 – 75% of all sex offenders who collect and/or possess child sexual abuse images also eventually commit contact offences against children.[7]

[7] Hernandez, Andres. (2000). "Self-reported contact sexual offenses by participants in the Federal Bureau of Prisons' sex offender treatment program: Implications for Internet sex offenders." Presented at the 19th Annual Research and Treatment Conference of the Association for the Treatment of Sexual Abusers, San Diego, California; Wolak, Janis, Finkelhor, David, and Mitchell, Kimberly J. (2005). "Child-pornography

The inability of ICE Units to begin to investigate many of these reports to determine which of those offenders are currently sexually assaulting children creates a substantial risk for some of the most vulnerable members of Canadian society. A U.S. study on possessors of child sexual abuse images found that the majority (83%) of offenders possessed images depicting children aged 6 to 12 years, and nearly 20% of offenders possessed images depicting children under 3 years of age.[8] Even if it were reasonable to expect these victims to ask for help, this study shows that many victims are too young to call for help. The IP address, captured during the commission of the crime, may be their only possibility for rescue.

An interesting comparison can be made between the tools available to police to respond to a report of a dangerous driver on real-world roads versus a report of a sex offender operating on the virtual highway known as the Internet. NCECC would like to suggest that an IP or email address is similar to a license plate and, therefore, police should have the same immediate capability to identify a person posing a public safety threat on the Internet as they do to identify such a threat on our roadways.

In a report of an impaired driver the primary objective is to intercept the vehicle before death, injury or property damage occurs. If police have license plate information for the suspect vehicle they have instant access to the address of the registered owner of the vehicle.

The registered owner's name does not identify the person in control of the vehicle. It may be stolen, sold or borrowed. The plate itself could be stolen. However, police will attend the location near the last known address of the registered owner and backtrack to the last sighting of the reported vehicle in an attempt to intercept the vehicle before harm is done.

It is NCECC's view that a license plate is similar to an Internet Protocol address. It is only a means to identify the source of a threat and to initiate an investigation. But in online child exploitation cases the IP address is the only means. There is only one source for this information -- a single ISP -- and IP information is perishable as data is purged regularly and often within four hours of online use. The ISP is the only possible source for the name and address of the registered account owner and, like a vehicle, the account holder information will not identify the person operating the Internet account at the time of the offence. Once a starting point is obtained, considerable investigational steps will follow including but not limited to database checks, CPIC, and physical surveillance of the residence. Once sufficient evidence exists, a search warrant for the residence

---

possessors arrested in Internet-related crimes: Findings from the National Juvenile Online Victimization study." National Center for Missing and Exploited Children. Alexandria, VA.

[8] Wolak, Janis, Finkelhor, David, and Mitchell, Kimberly J. (2005). "Child-pornography possessors arrested in Internet-related crimes: Findings from the National Juvenile Online Victimization study." National Center for Missing and Exploited Children. Alexandria, VA.

computer will be requested. If evidence is located during the search, and the perpetrator is identified, then charges can be laid.

7. ISP obligations

All major Canadian ISPs and some smaller ISPs researched by the NCECC have clauses in their customer agreements that prohibit the use of their networks to commit crimes and, often, they further state that they will cooperate with the police. Some explicitly state that if the system is used for child pornography they will cooperate with police. Therefore, it is not contrary to their customers' expectations if they cooperate. Yet they are still reluctant to do so.

ISPs in Canada claim they are simply a conduit and not responsible for the content on their systems or their customers' actions. Nevertheless, the NCECC would suggest that most other businesses expect their customers to act within the law and they take measures to protect their businesses from unlawful activities, so that if their business or their customers are affected by another customer's unlawful actions they can stop it, in collaboration with police.

For example, compare the business of an Internet Service Provider to a restaurant business. Each owner provides a service in exchange for compensation. As with the ISP, the restaurant owner does not care about his customer's personal habits (e.g., if a male customer is with his own wife or someone else's), nor does he care whether that customer is spending his very last dollar there. The restaurant owner must however, ensure that the customer's behaviour does not impact upon the other customers -- if he becomes abusive or obnoxious, the owner would ask him to leave. He must ensure that the customer is not over-served alcohol and if he appears to be intoxicated, the owner will ensure that he does not drive away by calling a taxi or the police. If the customer commits other crimes such as failing to pay for the meal, or attempts to use a stolen credit card, or starts a fist fight with someone in the restaurant, one can be fairly certain the restaurant owner would call police and would assist the police in identifying the customer. If police arrived unexpectedly and advised that a previous customer was suspected in the sexual assault of a child, the restaurant owner would provide all assistance possible. Somehow the reality of the child at risk seems to impact the restaurant owner far more than some ISPs.

In contrast, an ISP's customer may prey on children by luring, grooming or extorting them; send them live broadcasts of his masturbation; sexually assault children and share the sexual abuse images online; promote adult-child sex. Yet, unlike the restaurant owner who understands the link between what is happening on his premises and real crime and will call police if a problem arises, some ISPs apparently are neither on the look-out for crimes that may be occurring there nor do they report crime detected on their facilities. RCMP records show that the RCMP has only ever received one report of suspected online child exploitation from an ISP. Furthermore, when an ISP is approached by police regarding illegal activity involving a customer/ sex offender, who is using its

network or services, and when the ISP is asked to assist in many instances, as already discussed, such requests are being refused.

It may be that part of the explanation for the differences noted here is that ISPs are not a heavily regulated sector in comparison to food services which are well-regulated. However, from a policing perspective, rules (in the form of legislation) are needed to clarify for all ISPs and other telecommunications service providers that certain customer identifying information must be provided to police upon request, in the interest of public safety.

8. Statistics supporting the need for legislative response

Statistics for the number of telephone and Internet company refusals to provide basic customer identifying information is not being collected across all sectors of policing operations. Currently, only the NCECC is collecting this data. Since CCAICE instituted the current administrative model NCECC has had some success obtaining certain customer information from certain ISPs. However, this model is only used in cases of Internet facilitated child exploitation. Consequently, the RCMP is confident the percentage of refusals, if they were recorded in other areas of RCMP operations, would be even higher than the percentage of refusals that NCECC has noted. .

Results vary from this voluntary administrative process, whereby Internet child exploitation (ICE) investigators can request CNA information from ISPs , but the average over the past six months is that 33% of NCECC requests produce unsuccessful results. One third of all leads are concluded without investigation. The reasons are documented as refusals, lack of response or insufficient data retention times. The NCECC has now asked all major ICE units from BC, Alberta, Manitoba, Quebec, Ontario, Nova Scotia and New Brunswick to begin to log this data and to provide NCECC with their results.

NCECC Statistics for Customer Name and Address Requests and Results

2007 NCECC Requests	**ISP Response Summary**
March	***44% non-compliance***
April	384 requests made 164 refusals ***42% non-compliance***
May	***33% non-compliance***
June	125 requests 27 refusals ***21% non-compliance***
July	49 requests 16 refusals ***32% non-compliance***

August	62 requests 17 refusals ***27% non-compliance***

s.16(1)(a)i)

Specific Examples from International Cases

International case involving 78 Canadian IP addresses linked to the purchase of child pornography. Requests for information were submitted to the relevant ISPs and CNA information was provided for only 44 IP addresses. Cases sent to 16 jurisdictions (multiple customers per jurisdiction). To date, there have already been several arrests and charges for possession and accessing.
34 customers remain unidentified due to ISP non-cooperation. In some cases the ISPs did not respond, 18 refused to provide information and others reported that CNA was unavailable due to insufficient data retention periods.

International case involving 255 Canadian IP addresses linked to the purchase of child pornography. Requests were submitted and CNA was provided for 98 customers which were then forwarded to the police of jurisdiction.
157 customers remain unidentified due to ISP non-cooperation (35 refusals, lack of response or insufficient retention times).

International case involving 88 Canadian IP addresses linked to the purchase of child pornography. Requests were submitted, CNA was provided for 51. Files sent to 16 jurisdictions. To date, 3 arrests have been made for possession, accessing and distribution.
37 customers remain unidentified due to ISP non-compliance (12 refusals, lack of response or insufficient retention times)

Summary of the lack of cooperation in
June 26, 2007 - 2 requests for CNA forwarded to an ISP, one for an IP address and one for an e-mail. The ISP was advised that the information indicated that children were at risk. The ISP responded that information would be released only upon receipt of a production order. NCECC Investigator and Supervisor spoke to ISP representative and explained the urgency and provided all legal background on issue.
June 27 - ISP provided city and province only.
June 28 - the NCECC re-requested the customer name and street address so that potential child victims could be located and removed from harm. NCECC notified the law enforcement agency of jurisdiction.
June 29 - the local law enforcement agency contacted NCECC to advise that they were in contact with counsel for Child Services who would be in contact with the ISP, to resolve

this issue as there was a possibility of children at risk. The ISP remained unwilling to cooperate without a production order.
June 29 - NCECC was contacted by the ISP and advised that they were not willing to subject their subscriber to being "falsely accused or investigated." NCECC notified the child protection authorities in the city due to the risk to the child. The ISP reported being "pressured" by Child Services to supply the information, which they eventually did. The suspect had moved from the address finally provided by the ISP and was alerted by his ex-roommate of police interest. His computer had been dismantled into hundreds of pieces prior to police arrival to avoid forensic analysis.

Results of Cooperation

In cases where ISPs do respond positively to NCECC requests, positive results have been achieved. For example, as a result of an ISP cooperating and providing CNA information to investigators, a BC law enforcement agency was able to further their investigation to the point where they were able to obtain a search warrant for the suspect residence. The house search revealed an access door to a rooftop room containing a tripod set up with view of a schoolyard, swimming pool and trampoline next door. Items seized included child pornography, as well as videos depicting images taken up the skirts of women at a local mall, firearms, and other contraband.

9. Public support for police efforts

The NCECC believes that if the Canadian public had fuller knowledge of the challenges police are facing obtaining basic customer identifying information from ISPs, and the potential effect an ISP's refusal can have on effective law enforcement, the overwhelming majority of Canadians would be fully supportive of legislative proposals that would compel telecommunications service providers to provide this information to police, subject to reasonable privacy safeguards.

The NCECC is concerned that inaccurate and negative portrayal of the "customer name and address" issue in some media reports has left Canadians with a distorted view of the legislative proposals. The proposals would not compel telecommunications services providers to give police sensitive personal information without a warrant. Police are not seeking to obtain information without a warrant, where a warrant is normally required. That information would not be admissible in court and therefore useless to investigators.

The RCMP notes that Public Safety Canada's "Customer Name and Address Consultation Document" indicated that "options based on an administrative model are being considered" and it proposed that "a number of safeguards could be included under a possible administrative model requiring the release of limited basic CNA information to law enforcement". The RCMP supports the proposal for an administrative model, based in legislation that would include provisions to safeguard the privacy of this customer information and protect it from misuse. The RCMP hopes that with broader and more transparent consultations, the public debate may become more informed and the public criticism may decrease. The RCMP believes with a greater appreciation for the CNA

issue and the proposed legislative solution, a majority of the public would support these proposals.

PART TWO:
THE ADMINISTRATIVE MODEL AS A REASONABLE SOLUTION

The RCMP believes that in Canada, a reasonable, balanced, effective, well-regulated and accountable solution is needed for police to obtain basic customer identifying information to protect the public interest in safety, security and the suppression of crime while safeguarding individual privacy interests. In the RCMP's view this objective could be accomplished by the proposals for legislation that would establish the administrative model and build in solid, privacy-related safeguards. If one looks to the American example, one will find their Administrative Subpoena, which is issued by police, to be a similar type of administrative solution for obtaining this type of information.

Field Cod

The RCMP notes that in past consultations some participants have commented on the lack of publicly available information describing what a legislated administrative model could achieve. While Public Safety Canada's consultation document outlines that an administrative model is under consideration and summarizes general safeguards that could be incorporated in legislation, it does not provide a detailed picture of what a possible legislated framework could feature.

On the other hand, the RCMP notes that some detailed examples are publicly available online and they offer a clear picture of what such a model could entail. In Canada legislative proposals have been developed and tabled in the House of Commons as Bill C-74 in November 2005 and revived and re-packaged as a Private Member's Bill (Bill C-416), which received first reading in March 2007.

Therefore, in this part of the submission, the RCMP will be referring to provisions in these bills simply because, to date, they offer the most detailed examples to be found in the public domain that illustrate in concrete form what a legislated administrative model could encompass. By referring to actual provisions found in proposed legislation, the RCMP can explain more fully how, in its view, a legislated administrative model could provide a reasonable, balanced, and effective solution to the "CNA problem", within a well-regulated and accountable system.

By commenting on specific legislative proposals that now exist in the public domain, our purpose is not to champion any particular bills. What legislation would be most suitable and would be supported by Canadians is political matter for elected law-makers to determine. Rather reference to certain provisions in these bills will be made to highlight in a concrete (less theoretical and more practical) way how legislation could be used to resolve the CNA issue, meet important public policy objectives, and balance public interests at the same time.

1. **Requests would be in writing and otherwise governed by legislation**

The proposed legislative model could require telephone companies and Internet service providers to give a police officer some basic customer identifying information only when a police officer approaches them with one or two pieces of basic customer identifying information and requests in writing additional related subscriber identifying information (see for example Bill C-416, clauses 17(1) and 31(1)(e)). In other words, police would need to already have obtained some customer identifying information through open or other lawful sources before approaching a service provider with a request. For example, police may have a customer's name and need to find out from the service provider the residential address for that customer. Alternatively, as often arises in Internet child exploitation investigations, police may have an IP address, as well as a date and time that an unidentified user was online, and they may need to find out, from the ISP to whom that IP address belongs, who the account holder is and his or her address.

2. **Rules for the collection, use and disclosure of subscriber information would be set out in and governed by legislation**

Various other legislative controls could be established through the proposed legislative model, to regulate and limit who can make a request and for what purposes (see for example clauses 17(2) to (5)).

A police officer making a request would only be able to do so if he is performing a duty or function of a police service, including any functions related to the enforcement of Canadian laws (see for example clause 17(2)(b)).

Only a percentage of a police service's employees would be able to make requests (see for example clause 17(4)). Furthermore, these requestors would be required to keep records and adopt measures to protect the privacy of that information that would be set out in specific detail in regulations made under the legislation (see for example clause 17(6)).

The records kept and practices followed in making requests to ISPs and telephone companies would be subject to internal audits (see for example clause 20(1)). In addition, for the RCMP, the proposed legislative model could require that any results of an RCMP internal audit that ought to be brought to the attention of the Minister responsible for the legislation would be reported to the Minister (see for example clause 20(2)).

To include additional, independent oversight, the RCMP could be required to provide a copy of that report to the Privacy Commissioner of Canada (see for example clause 20(3)). The Privacy Commissioner could be given the express power to conduct an audit of the CNA information practices of the RCMP to ensure compliance with the statutory rules governing these requests (see for example clause 20(4)).

Based on these concrete examples of the types of requirements, privacy safeguards, and accountability measures that a legislated administrative model could encompass, the RCMP is satisfied that such a model could serve to make it clear for everyone (police agencies, telephone and Internet companies and their customers):

- when service providers must help the police by providing them with basic customer identifying information;
- exactly who is authorized under the law to ask service providers for such information and that these persons are to be limited in number;
- precisely what customer identifying information the law will allow police to request and for what purposes;
- how the police will have to submit their request to a company (e.g., in writing so an audit trail is created);
- how the information must be treated by the requestor once the telephone company or ISP releases it so that it is not misused and it continues to be properly protected; and
- how the police's information handling practices for any information received by request from a service provider will be overseen (e.g. through mandatory internal audits and additional external audits at the discretion of independent officials such as the Privacy Commissioner of Canada).

3. Advantages of the legislative model

Although such a legislated administrative model would not involve police in seeking a warrant or a court order for the information in question, a reasonable and accountable process for lawfully obtaining this information could be established, regulated and administered under federal legislation. It is important to emphasize that a legislated regime for police to obtain certain customer information without having to obtain the prior approval of a court official does not mean police would have unbridled access to the information in question. It does mean that police requests for customer identifying information would be well-regulated and that Parliament could ensure privacy interests, as well as other public interests, would be fostered using this model.

Furthermore, the legislation would impose a clear legal requirement on telecommunications service providers to provide certain customer information to police when it is requested pursuant to the legislation. Such a requirement should satisfy the companies' liability concerns and eliminate the problems police face with service providers who currently choose not to cooperate with police.

The checks and balances would be in statute rather than falling to the courts to administer through the oversight they exercise in considering warrant applications. However, the authority for police to obtain the information and the controls over the request process would be entrenched in law with appropriate oversight and accountability built into the legislation.

Furthermore, since this legislative model would not require police to make applications to a court official (such as a Justice of the Peace) but rather would require police to submit

written requests for the information to service providers, this process would not place new demands on an already over-burdened court system.

CONCLUDING REMARKS

The RCMP is satisfied that if Parliament were to legislate an administrative model to govern police requests to obtain identifying information for telephone and ISP customers, the type and amount of protection provided through such legislation would be reasonable and would meet public policy objectives while being proportional with the level of privacy that the public expects lawmakers to give this type of basic (non-intimate) customer identifying information.

The RCMP does not believe the same objectives could be accomplished as effectively through some type of new warrant that could be created in legislation.

The RCMP is grateful for having been given the opportunity to express its views on the issues associated with police seeking reasonable, lawful and effective access to customer identifying information.

NCECC Comment on Lawful Access

The Government of Canada's primary responsibilities include:

- ensuring the safety and security of its citizens;
- balancing this priority with the rights and freedoms of individual citizens; and,
- assessing emerging risks to make certain that adequate protective measures are in place.

The Internet has created significant risks to adult financial integrity and the personal safety and security of children and these risks challenge the ability of the Canadian Government to uphold its primary responsibilities as outlined above. No protective measures have been implemented to protect Canadian children. The unacceptable delay for protective measures has been greatly influenced by financial interests. In essence, the safety and security of children has not been prioritized.

Why a Warrant is not an option.

1. A search warrant cannot be granted if there is no search.

*R.*v.*Quinn* – court ruled that obtaining customer name and address from an account number is not a search.
Further precedents that no there is no reasonable expectation for privacy attributed to customer name and address (*R* v. *Plant*, *R* v. *Lillico*)

2. Warrants cannot be obtained at this stage of an investigation.

A request for name and address related to an Internet account indicates only who is financially responsible for the account. Numerous investigative steps must be taken to determine who accessed the computer and who may be responsible for the crime. A warrant may be obtained once police form reasonable and probable grounds as to who may be culpable and determine where evidence is likely to be found.

In the case of child sexual exploitation offences in Canada, the investigation normally begins when a seizure of evidence from one offender reveals an Internet Protocal (IP) addresses of other offenders who have uploaded, downloaded, shared (etc) child pornography. When computers "speak" to each other, the IP address is automatically captured, similar to a long distance telephone bill. Police then commence a new and separate investigation to identify those responsible. The investigation begins, and often ends, with an IP address. Police must ask the ISP for the customer name and address associated to each IP address. At the time of the request, police are operating on unsubstantiated information (suspicion) in an investigative process that may or may not establish reasonable grounds. This is sometimes referred to the "pre-warrant stage" of an investigation. A warrant cannot be obtained unless reasonable and probable grounds exist.

Example: Dawson College, Montreal.

Prior to the shooting, there was no information that the suspect had committed any offence. If his postings on the Internet of himself with a firearm had been located prior to the incident, the investigation at that point would be a proactive - preventative action dependent on the ability of the police to identify suspicious behaviour and investigate to determine the level of risk/danger. This is a critical public safety responsibility assigned to police.

If police had requested a name and address from the ISP, it is likely the request would have been refused. There are no warrant provisions to allow the police to initiate this process and the file would have been concluded and the incident occurred anyway.

Had the police been alerted and had the ISP provided the name and address, investigators could have determined if he had a firearms license and if he had any registered firearms. A face-to-face interview would have provided the police the opportunity to evaluate the level of risk he posed, seize the weapons, and ensure access to mental health professionals. The homicide, suicide, injuries, and public distress could have been prevented largely based on the provision of non-biographical information.

Many cases such as criminal harassment, hate crimes, and threatening have the potential to result in death or other injury however warrants would not be possible at the outset of many of these investigations.

Several police responsibilities in assisting the public, while part of their core responsibilities, do not involve the investigation of crimes but do involve needing to identify people. As a result warrants are not obtainable. Examples include but are not limited to notification of next of kin; investigation of reports of overdue hunters/hikers; search and rescue for missing persons; and, assistance to individuals apprehended under mental health act or assistance to Coroner in the identification of deceased persons.

3. Police are not requesting information which has a reasonable expectation of privacy.

Judicial authorizations are designed to protect people's reasonable expectation of privacy, whether it is the sanctity of places where an individual has this expectation (for example, home, office) or information that attracts this expectation (for example an individual's core biographical information such as DNA, medical records, chat logs, and tracking of websites visited). A warrant is required to obtain this *core biographical information*.

Warrants are not required to access *non-core biographical information*. A person's name, address, and phone number, are *not* core biographical information. In addition, once information is available through other publicly accessible means, it is no longer considered to be confidential. Names and addresses are available through numerous other avenues (for example, phone book, property records, driver's license, vehicle registration).

4. It is inappropriate use of judicial process when companies, not the law, dictate the use of warrants.

Law enforcement investigating child sexual exploitation are often forced into preparing warrants to obtain information in circumstances where authorizations are not required by law, but rather in response to ISP's that are not willing to assist. Faced with a choice between saving a child enduring sexual abuse or setting poor precedents, the police have no choice but to capitulate. This is an inappropriate and irresponsible waste of finite police and judicial resources. It is not required by law and serves only to provide ISP's with a level of comfort.

The ISP industry is unique in demanding warrants for this type of basic customer information before assisting an investigation. Many other companies willingly assist police in similar circumstances to further their work in the prevention, detection, and early stages of investigation of crimes.

Although telephone companies have voluntarily assisted police in the past, and today a majority of telephone and ISP's provide this basic identifying information to police, there is an emerging reluctance to voluntarily provide this type of information to police. Companies suggest they are concerned with being held liable under privacy laws for disclosing this information without the customer's knowledge or permission – they are generally not prepared to take what they have deemed to be a legal risk to assist, except (but not always) in life and death situations. In cases of child sexual exploitation offences there is no definitive way to assess level of risk to the child until an investigation is undertaken.

Continued demands for warrants in situations where none are required will no doubt result in additional requests for warrants prior to cooperating with the police. In cases where an ISP's customer is committing an offence using the ISP network, at the very least the ISP is a witness. It could be argued that they are obstructing the investigation of an offence by demanding a warrant for "pre-warrant" information and refusing to cooperate with police. ISP's staunchly defend against this assertion by claiming that they are merely a conduit and that they have no knowledge of or control over what passes through their networks. However, once an investigator contacts an ISP and provides notification that an offence is being facilitated via their networks, the company can no longer claim ignorance.

5. Time delay, resource impact, consequences to the victims.

The NCECC alone makes approximately 200 requests to ISPs per month for customer name and address information. All Internet child exploitation (ICE) investigations make these requests. The time to complete a warrant, locate and drive to a JP (which is often not in close proximity), wait for the approval, and repeat this process would be an immense burden on police across Canada. More importantly, finite police resources dedicated to identifying and locating victims would be severely depleted as investigators

Canadian Police Association
L'Association canadienne des policiers et policières
100-141, rue Catherine Street
Ottawa, Ontario K2P 1C3
Tel: (613) 231-4168 Fax: (613) 231-3234
Internet: www.cpa-acp.ca *E-mail/Courriel*: info@cpa-acp.ca

...not allow for this concentration. In addition, while this unnecessary ...ged the investigator is aware that the abuse of the child could be ongoing.

6. Public Expectation of Police

The public expects the police to investigate crimes and keep citizens safe. With the exception of the Internet, in every other domain where there is a potential for crime or harm, there exists a capacity for police to rapidly investigate alleged offences. If the public were aware of the serious harm and suffering that child victims experience in respect to these offences they would demand that everyone do everything possible to prevent, detect, and end these horrible crimes against children. It is hard to imagine that the public would want privacy protection for non-core biographical information to trump the safety and well-being of children in these circumstances.

Example: Impaired Driving

In a report of an impaired driver fleeing a fatal accident, police have instant access to identify the registered owner of the suspect vehicles. The process of identifying the owner of a vehicle from a license plate is only one investigational step. A registered owner is not necessarily the operator at the time of any alleged infraction. The customer name does not identify the person in control of the vehicle at any given time. Police will attend the last known address to make enquiries and attempt to intercept the suspect vehicle.

A license plate is similar to an Internet Protocol address. It is the only means to initiate an investigation and to begin to identify the perpetrator. The information is perishable as data is purged regularly often within hours. The ISP is the only possible source for the name and address of the registered account owner and, like a vehicle, will not identify the person operating the Internet account at the time of the offence. Once a starting point is obtained, considerable investigational steps will follow including but not limited to database checks, CPIC, and physical surveillance of the residence. If evidence exists, a search warrant for the residence computer will be requested. If evidence is located during the search, and the perpetrator identified, charges may be laid.

Without customer name and address information, an investigation into the abuse of a child by a potential sex offender is concluded. Several studies indicates that between 30 – 55% of all sex offenders who collect and/or possess child sexual abuse images also commit contact offences against children. The inability to investigate these reports to determine which of those offenders are currently sexually assaulting children on and off the Internet is unacceptable to investigators and would shock the Canadian public.

The RCMP also believes that the public is right to expect police to be conscientious and accountable in handling any personal information they obtain – whether voluntarily or under a court order and whether that information is highly sensitive personal information (such as a person's DNA) or information that attracts little or no privacy interests, such as one's name, telephone address, and home address.

7. Public Expectation of ISP's

The public expects and assumes that ISP's readily assist police particularly in investigations involving children. They would be appalled to learn the facts.

For example, if parents suspect their missing 10 year old daughter has gone to meet Johnnie4@BigISP.ca and they call police for assistance in locating her and if BigISP won't voluntarily give police the name and stress address associated with the email address of Johnnie4 then their efforts to try to locate their child are thwarted. This is not an investigation where a warrant would be possible. It is an investigation where time is of the essence and where public expectations are high.

8. Court Expectations of ISP's

Precedents exist which indicate that as much as citizens are expected to report crime and participate in the criminal justice process, so is the expectation for corporations and citizens who may be the only witness to criminal acts.

9. Oversight

In addition to internal and external police complaint processes, the Privacy Commissioner and other regulatory bodies, Crown counsel review all criminal charges proposed by the police. The courts have the ultimate oversight authority and will ensure evidence collected is obtained in accordance with the law.

10. Public Tolerance

Public support for police to investigate and protect children is very high. One need only look at examples of missing children and how the public cooperates in police efforts in those cases to know that public support is strong. The public would likely support ISP cooperation in exchange for rescuing children from child sexual abuse. If there was knowledge of the challenges police are facing rather than the misinformation about what police are seeking to do, such as false claims that the police want to monitor private Internet activities without a warrant, this support would be forthcoming.

11. Victims

Evidence of child sexual abuse reveals that the majority of victims are under 9, many are under 6 and 20% are under 3. Most are too young to call for help. The IP address captured during the commission of the crime, is the only possibility for rescue.

12. Statistics

Statistics for the number of telephone and Internet company refusals to provide basic customer identifying information is not being collected across all sectors of policing

operations; but, based on anecdotal information the RCMP believes the percentage of refusals would be higher in other fields. There is a voluntary administrative process in place however results are as indicated below and this process is only applicable in cases of child sexual abuse investigation, if ISP's cooperate at all. The NCECC has now asked all major ICE units to provide statistics.

NCECC Statistics for Law Enforcement Requests for Customer Name and Address

2007 Law Enforcement Requests	**ISP Response Summary**
March	***44% non-compliance***
April	384 requests made 164 refusals ***42% non-compliance***
May	***33% non-compliance***
June	125 requests 27 refusals ***21% non-compliance***
July	49 requests 16 refusals ***32% non-compliance***
August	62 requests 17 refusals ***27% non-compliance***

s.16(1)(a)i)

Examples

[redacted] Multiple IP's on this case.
78 Requests submitted, CNA was provided for 44 IP's. Cases sent to 16 jurisdictions. Several arrests and charges to date for possession and accessing.
34 customers remain unidentified due to ISP non-compliance. In some cases the ISP's did not respond, 18 refused and others reported CNA unavailable due to insufficient data retention periods.

[redacted]
255 Requests submitted, CNA was provided for 98 customers, sent to police of jurisdiction. Recent investigation so no results from agencies to date.
157 customers remain unidentified due to ISP non-compliance (35 refusals, lack of response or insufficient retention times)

[redacted]
88 Requests submitted, CNA was provided for 51. Files sent to 16 jurisdictions. To date, 3 arrests have been made for possession, accessing and distribution.
37 customers remain unidentified due to ISP non-compliance (12 refusals, lack of response or insufficient retention times)

1) Detailed Examples:
June 26, 2007 - 2 requests for CNA forwarded to an ISP, one for an IP address and one for an e-mail. The ISP was advised that the information indicated that children were at risk. The ISP responded that information would be released only upon receipt of a production order. NCECC Investigator and Supervisor spoke to ISP representative and explained the urgency and provided all legal background on issue.
June 27 - ISP provided city and province only.
June 28 - the NCECC re-requested the customer name and street address so that potential child victims could be located and removed from harm. NCECC notified the law enforcement agency of jurisdiction.
June 29 - the local law enforcement agency contacted NCECC to advise that they were in contact with counsel for Child Services who would be in contact with the ISP, to resolve this issue as there was a possibility of children at risk. The ISP remained unwilling to co-operate without a production order.
June 29 - NCECC was contacted by the ISP and advised that they were not willing to subject their subscriber to being "falsely accused or investigated." The ISP reported being "pressured "by Child Services to supply the information, which they finally did on June 29. The suspect had moved from the address finally provided by the ISP and was alerted by his ex-roommate of police interest. His computer had been dismantled into hundreds of pieces prior to police arrival to avoid forensic analysis.

Results of Cooperation

Recent case on Vancouver Island, B.C. Local law enforcement completed their investigation and obtained a search warrant for the residence. House search revealed an access door to a rooftop room containing a tripod set up with view of a schoolyard, swimming pool and trampoline next door. Items seized included child pornography as well as videos depicting images taken up the skirts of women at the mall, firearms, and other contraband.

Infomart SPECIAL EDITION
straight to the point

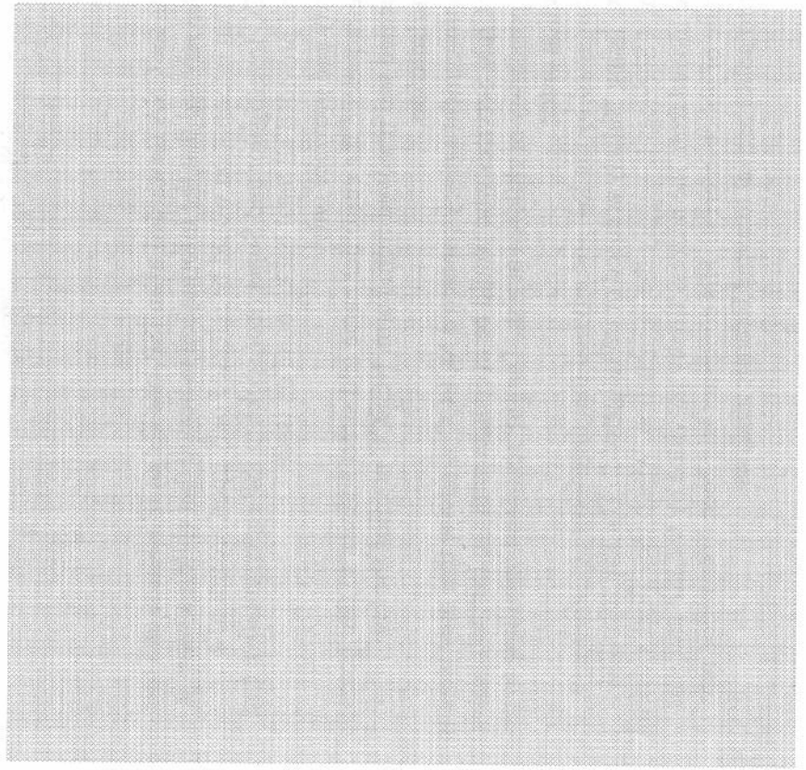
EDMONTON JOURNAL

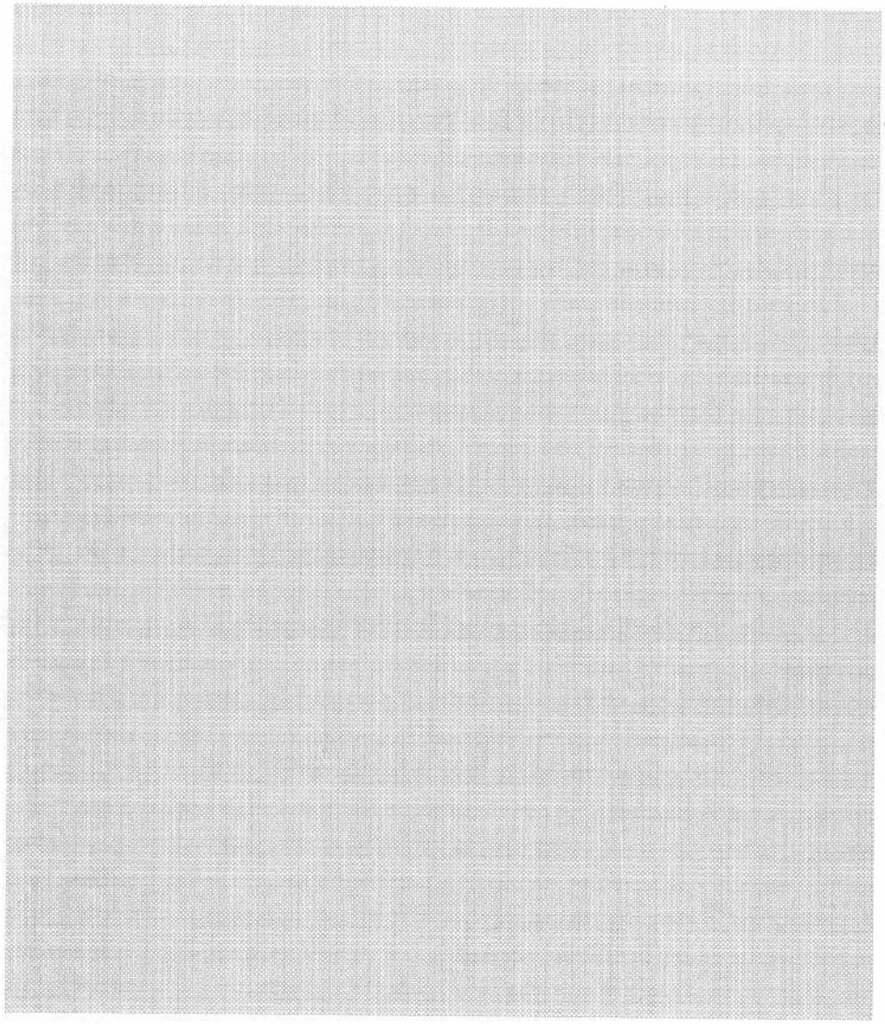
Church helps when pedophiles feel weak

The Edmonton Journal
Sun 17 Jun 2001
City
B3
Crime

Hanneke Brooymans, Journal Staff Writer

s.68(a)





FINAL
Edmonton
The Edmonton Journal

http://specialedition.net/cgi/se4.cgi/ssullivan/3135/pq/print/21160/20010617/all/2618/ 6/17/2001

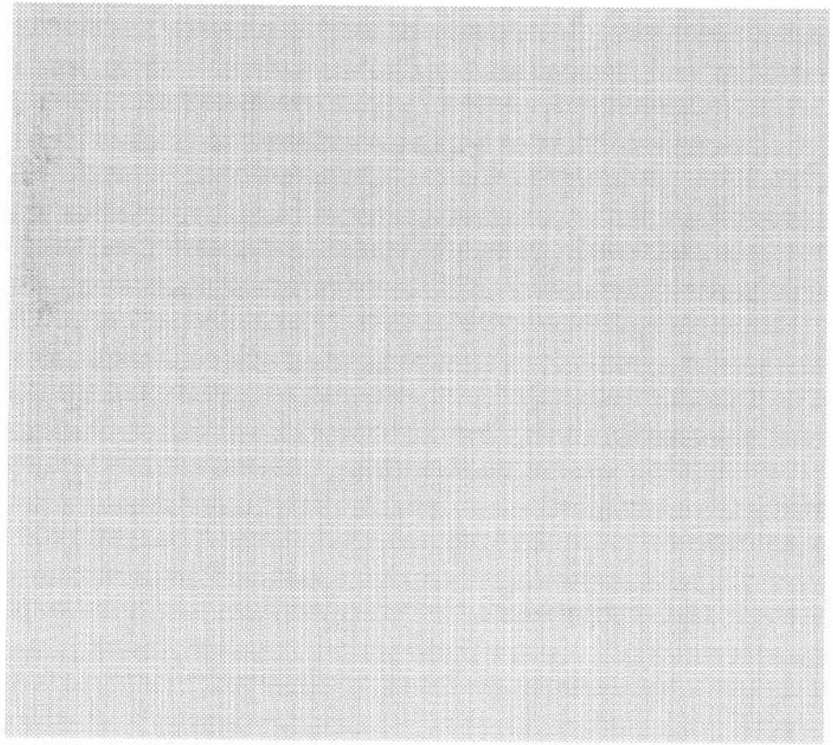
Infomart SPECIAL EDITION
straight to the point

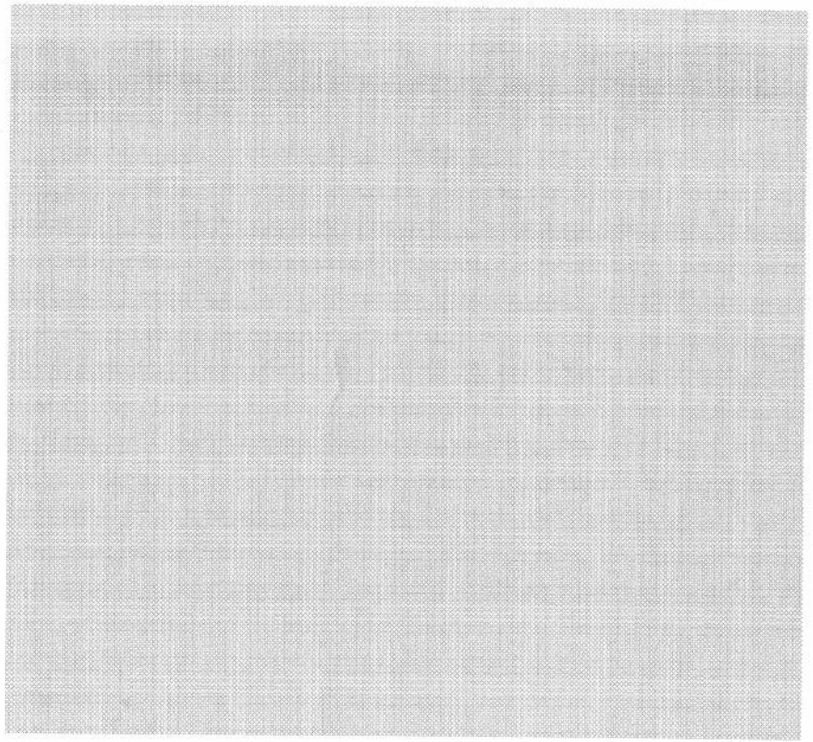
SUN

'IMPULSES WILL ALWAYS BE THERE, BUT I CAN CONTROL IT'

The Ottawa Sun
Sat 16 Jun 2001
News
18
BY KATHLEEN HARRIS, OTTAWA SUN

s.68(a)





Final