Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Royal Canadian Mounted Police
Commissioner

Gendarmerie royale du Canada
Commissaire

Guided by Integrity, Honesty, Professionalism, Compassion, Respect and Accountability

Les valeurs de la GRC reposent sur l'intégrité, l'honnêteté,
le professionnalisme, la compassion, le respect et la responsabilisation

Protected "B"

The Honourable Stockwell Day, P.C., M.P.
Minister of Public Safety
269 Laurier Avenue West
Ottawa, Ontario
K1A 0P8

Dear Mr. Day:

As you are aware, the RCMP has supported the Government in the preparation of legislative proposals for the federal government's Lawful Access initiative, in particular, the shaping of proposals that you, as Minister of Public Safety, would introduce in a stand-alone lawful access bill.

I am writing to express our strong support for both the interception capability and subscriber information aspects of the current legislative proposal. It has come to my attention that these may be separated and that only the portion of the bill related to interception capability will be forwarded to Government. It is the position of the RCMP that both elements are essential to our public safety mandate, and would urge that the bill not be separated. I recognize that further review of the subscriber information could introduce delay in the tabling of the bill. If that is the case, the RCMP would support removal of the subscriber information component in the interests of moving forward with the rest of the bill without further delay. However, should this be your direction, I would respectfully urge that a legislative solution to the challenges with subscriber information remain a top priority.

The RCMP's National Child Exploitation Coordination Centre (NCECC) submitted a document entitled *Customer Name and Address Information Consultation (October 2007)* to the Public Safety and Industry Canada Consultation Panel. An Executive Summary is enclosed. It offers the most detailed explanation, to date, of the problems that the RCMP and Canadian police in general face in obtaining basic, non-sensitive customer information from Internet Service Providers (ISPs) and telephone companies. It also outlines the negative impact this has on law enforcement efforts to maintain public safety, and supports an administrative/regulatory model which provides a reasonable and balanced solution that merits full public consideration.

.../2

1200 Vanier Parkway
Ottawa, Ontario
K1A 0R2

1200, promenade Vanier
Ottawa (Ontario)
K1A 0R2

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The NCECC submission demonstrates that the information in question is not sufficiently sensitive to require a warrant, and that the controversy over "CNA" (customer name and address) information has been miscast by the media. The pertinent public policy issue is how lawmakers can enable police to obtain that information while safeguarding individual privacy interests.

In cases where they have an IP address that was used or have found a cell phone at a crime scene, police are seeking to obtain the name or address of an unidentified customer from ISPs and/or telephone companies. An ISP or telephone company response indicates only who is responsible for, or is registered to the account, much the same as a license plate on a motor vehicle identifies the owner.

Obtaining a warrant for CNA information is not necessary under the law. In fact, the Supreme Court of Canada affirmed (in the *Plant* and *Tessling* cases) that a person's non-core biographical information does not attract a reasonable expectation of privacy. Therefore, it does not require the prior oversight and authorization of a court official for it to be released to police. Police recognize that CNA-type information is clearly personal information: personal information being any information that identifies a particular person. However, CNA personal information is not information that reveals intimate details about an individual and therefore its release to police does not need to be supervised by a court through a warrant process.

Furthermore, obtaining a warrant is not possible or practical in many cases. Obtaining warrants in the early stages of an investigation is not possible as police simply do not have sufficient grounds to apply for a warrant. In the performance of general policing duties, such as finding and notifying next of kin or locating overdue and missing family members, there is no criminal offence. Therefore, there are no grounds to apply for a warrant. Therefore, obtaining *timely* CNA information with a warrant in fast-moving, time-sensitive, or high CNA volume investigations, such as multi-million dollar Internet frauds, sexual assaults or other serious crimes in progress is not practical.

A warranted CNA regime would lead to tremendous strains on the judiciary and on law enforcement as telecommunication service providers process hundreds of thousands of CNA requests yearly.

.../3

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.13(1)(a)

s.16(1)(a)

s.16(1)(b)

Today, there are approximately 400 telecommunication service providers in Canada. Certain telephone companies, as well as ISPs, resist and regularly refuse to assist in this way. In this regard, the NCECC reports a 30% non-compliance rate with CNA requests. Statistics for non-child exploitation investigations are not available.

The following three real life examples highlight this concern:

47 unidentified persons violating children online in Canada

In a recent international child pornography investigation, [redacted] 28 countries where online child sexual exploitation was occurring. Two hundred (200) IP addresses associated with online child sex offenders using Canadian ISPs were sent to the RCMP in Canada to identify the location of these accounts. Once that basic information was obtained, investigators could then work to confirm the identity of the suspects and then obtain search warrants. Forty-seven of 200 requests made to ISPs were flatly refused. Those 47 leads reached a dead-end and could not be investigated, leaving the unfound victims vulnerable to further abuse and placing other children at risk.

Live, online child rapist identified with ISPs' help

[redacted] The investigator was able to summon help from the police of local jurisdiction who immediately went to the scene of the crime. If the investigator had been forced to seek a warrant to compel the ISP to provide the information, the little girl would have been raped again that night. Due to the cooperation of this ISP, police were able to rescue the girl without delay.

International Internet Fraud Investigation

Recently, the RCMP assisted [redacted] in identifying who was accessing unsecured wireless computer networks in Canada [redacted] in order to commit fraudulent activities against large U.S. corporations. The service providers

.../4

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

would not provide police with the CNA information they needed to pursue the investigation in a timely and efficient manner. As a result, it took eight full-time technical investigators five days to finally locate and arrest a number of suspects. Their attempted frauds were valued at $1 million, and they were unfortunately successful at actually defrauding victims of $15 million. The requirement to receive this information in "real-time" prevented investigators from obtaining warrants for the numerous IP addresses provided by the foreign agency to investigate. Had the requested CNA information been provided, investigators could have interrupted the criminal activity earlier and considerably reduced the financial harm of the fraud.

As demonstrated in the preceding scenarios, investigations are now being seriously delayed or thwarted due to non-compliance with CNA requests. Public safety risks of both personal injury and economic harm, will increase without a timely and workable solution to the CNA issue. The proposed CNA administrative scheme provides strong checks and balances for the protection of privacy. It would also develop national consistency in the handling of this information, and a process that would enable internal and independent audits of information handling practices.

In closing, I want to express my appreciation to you for considering the significant impact that this proposed legislation will have not only on police investigations, but on public safety. Should you wish to discuss this matter further, I remain available to meet with you or, if you prefer, RCMP officials may be made available to meet with your Department to discuss the CNA issue.

Yours sincerely,

for William J.S. Elliott ADD

Enclosure

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Questions and Answers

1. What is "CNA" information and why do police need it?

Answer: "CNA" stands for "customer name and address". In the telecommunications world, it is the name and street address of the person who subscribes to a telephone or Internet service. A request for CNA is often a starting point to follow an investigational lead. The address, phone number and name provided by the telephone or internet company informs police where they have to start looking to find and talk to victims, witnesses and suspects.

2. Why don't police just get a warrant when they want CNA information?

Answer: CNA is "personal information" that is not sensitive. It doesn't reveal intimate details about a person's life. The law doesn't require a warrant for this type of "tombstone" information. It is not information that the Supreme Court of Canada says police need a warrant for in order to obtain it legally. It would not be an effective use of police or court resources to require police to obtain warrants for information that is not sensitive enough to require a warrant. In addition, police can only obtain a warrant for the investigation of an actual offence. If they are carrying out general duties and no foul play is suspected--for example, trying to locate overdue hikers or a missing spouse--then applying for a warrant is not even possible.

3. Why don't ISPs and telephone companies cooperate and volunteer CNA information if a warrant is not required?

Answer: ISPs and telephone companies are subject to privacy legislation. There is a specific federal law that regulates how they must handle and protect their customers' "personal information". That law allows them to provide non-sensitive customer information to police. However, it does not require them to do so – this would require a statute or a court order. Without a legal obligation, or a court order to compel the provision of this information, companies are concerned about potential liability if information is provided voluntarily.

4. How many requests do police make for CNA and how many are refused?

Answer: Police do not track the number of these requests or refusals. There could be hundreds of thousands of such requests made in a year across Canada. Since April, 2007, the RCMP's National Child Exploitation Coordination Centre (NCECC) began to track the number of requests it makes to ISPs for CNA information and how many are refused. The number of requests per month has varied – in one month close to 400 requests were made and the next month the total was closer to 100. One-third of all CNA requests in child exploitation investigations are refused.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

5. Would the proposed legislation give police new powers so they could avoid getting a warrant?

Answer: No. The new law would clarify for ISPs, telephone companies, customers and police what basic, non-sensitive information will be provided if police need it to perform their investigative or general duties. This law would not give police the power to intercept communications or spy on internet use without a warrant.

6. Aside from Canadian police services, who supports the proposed legislation?

Answer: Public Safety and Industry Canada officials recently held public consultations on legislative proposals for an administrative model that would require Internet Service Providers (ISPs) and telephone companies to provide only basic, non-sensitive subscriber information to police when it is needed to help them try to identify people. Key stakeholders who participated in this most recent consultation process, including representatives of ISPs and telephone companies, as well as the Privacy Commissioner of Canada and the Federal Ombudsman for Victims of Crime, found the proposals to be reasonable and indicated support for them. Keeping the proposals as part of the Lawful Access bill would broaden public dialogue on this subject. The RCMP anticipates that most Canadians would welcome the opportunity for a more public and well-informed dialogue about the CNA challenges facing police. Their support of these proposals, which are reasonable and ultimately serve public interest, is essential.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

EXECUTIVE SUMMARY

NCECC – RCMP SUBMISSION TO PUBLIC SAFETY CANADA CUSTOMER NAME AND ADDRESS (CNA) INFORMATION CONSULTATION

The National Child Exploitation Coordination Centre (NCECC) of the RCMP participated in Public Safety and Industry Canada's recent public consultations concerning customer name and address (CNA). The main points of the NCECC submission, made on behalf of the RCMP, are summarized here.

Suitable legislation is essential to specify what customer identifying information Telecommunications Service Providers (TSPs) must provide to police upon request, as well as to ensure suitable privacy safeguards are in place for that information. Police have longstanding authority under the common law to ask people, including companies, questions in the lawful execution of their duties. But the common law does not require answers. Only legislation can compel TSPs to provide basic customer identifying information to police upon request.

While it is not standard practice in police operations to log instances where police requests to companies to voluntarily provide this information are turned down, NCECC recently began documenting such refusals to gauge the magnitude and impact of the problem. On average, one-third of all requests made each month to ISPs for basic CNA information are not being met. As a result, many child exploitation investigations never get off the ground, online offenders continue to offend and their child victims continue to suffer.

The debate surrounding police access to CNA in the media, so far, has concentrated on whether police should simply obtain a warrant. While, at first glance, this option might appear viable, it is not practical and would not serve law enforcement's operational needs or the public interest.

Police recognize that the information in question is "personal information"; however, it is not personal information that is sensitive. It does not reveal intimate details about someone's lifestyle and personal choices. The Supreme Court of Canada affirmed (in the *Plant* and *Tessling* cases) that a person's non-core biographical information does not attract a reasonable expectation of privacy and, therefore, does not require the prior oversight and authorization of a court official for it to be released to police.

Nonetheless, TSPs are often reluctant to volunteer CNA information. Some simply refuse to do so and tell police to obtain a warrant. To be able to continue their investigations, when police have sufficient information to obtain a warrant they will usually accede to the TSP's demand. On the other hand, applying for warrants, in situations where the law does not require them, appears to law enforcement agencies to be a poor use of limited police and court resources.

In cases, where the matter is in the early, "pre-warrant" stage of investigation, police simply do not have sufficient grounds to apply for a warrant. An ISP's refusal to

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

voluntarily provide a customer's name and address information at this stage of a child exploitation investigation often means the end of the investigation.

In addition, police do more than conduct investigations. They perform general duties -- such as finding and notifying next of kin or locating overdue and missing family members. Since general duties do not involve the investigation of an offence, at no time can a warrant be used to secure customer identifying information for these purposes.

Lastly, in addition to situations where obtaining a warrant for basic customer information is not at all possible, there are circumstances where obtaining a warrant is not feasible because the CNA information is needed immediately to prevent a serious harm from occurring. For example, an offender is inviting collaborators to watch him rape his step-daughter live on the Internet or an offender is accessing other people's non-secure wireless Internet connections to invisibly commit fraudulent financial transactions. In these circumstances, while police would be able to make out the grounds to obtain a warrant, by the time they would be able to do so, serious harm to a person or property would have occurred.

Considering the problems police encounter obtaining CNA voluntarily and the inadequacy of warrants as a solution, the RCMP and other police agencies have come to the conclusion that legislation is needed to oblige TSPs to provide basic customer identifying information upon request. This legislation must be administrative in nature – to accommodate all investigative and general policing reasons for seeking this information. Also it must incorporate various measures to safeguard privacy interests (such as detailing what information can be requested, who can request it, how it is to be recorded and handled), as well as to build in audit and accountability mechanisms.

Submission Prepared by:
Supt. Earla-Kim McColl
NCECC
In Collaboration with
Susan Alter, Counsel, RCMP Legal Services

27 October 2007

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

What exactly did the Minister say in the media?

Calgary Herald / CanWest News Service 14 September 2007

"We have not and we will not be proposing legislation to grant police the power to get information from Internet companies without a warrant. That's never been a proposal," Day told CanWest News Service Thursday. "It may make some investigations more difficult, but our expectation is rights to privacy are such that we do not plan nor will we have in place something that would allow the police to get that information."

CBC Radio One, 20 September 2007. 11:32 a.m. interview of Minister Day by Jesse Brown

Jesse Brown (Question): It [the consultation document] says,"Law enforcement agencies have been experiencing difficulties in consistently obtaining CNA information. Some companies provide the information voluntarily while others require a warrant. This poses a problem." So the question many people wrote in to ask is what other possible meaning can be derived from the wording of the document?
Stockwell Day (Answer): ...the Liberals tabled legislation ... that would allow that type of garnering of information without a warrant. ...[T]hat approach, the without-warrant approach is being supported by Stephane Dion. We are not supporting that.

Jesse Brown (Question): ...[T]here were a lot of comparisons to the Patriot Act and wiretapping. People are very concerned about this .... Can you assure the Canadian people that this issue of circumventing warrants for online information is now off the table for good?
Stockwell Day (Answer): We never put it there .... I hope that people understand that when we say we are not in any way, shape or form wanting extra powers for police to pursue items without a warrant, that is not what our purported legislation is going to be doing. That was previous Liberal legislation. That's not the path that we're walking down, at all.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

CUSTOMER NAME AND ADDRESS (CNA) 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

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

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.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

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

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

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.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

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.»

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

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. <u>Police are not requesting personal information that is confidential or sensitive</u>

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).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

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. s.13(1)(a)

For example, a recent child pornography case from [redacted]28 countries and within Canada over 200 IP addresses. Upon receipt, the NCECC attempted to identify the account holders. They were unable to identify the account holder information of 47 of the IP addresses due to the lack of ISP cooperation. 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.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

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

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

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. An example of this type of situation comes from a recent online fraud investigation. s.13(1)(a) s.13(1)(d) s.16(1)(a)

In September 2007, RCMP Special "I " assisted [redacted] The objective of this operational request was to identify the individual who was accessing unsecured wireless computer networks in Canada ("war

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

driving") in order to use other people's Internet access points to commit fraudulent activities against large U.S. corporations. s.13(1)(a) s.13(1)(d)

[redacted] s.16(1)(a)

[redacted] It was the responsibility of the RCMP to respond to reports [redacted] of unlawful network access in an effort to track down the location of the suspects. To do so, in real time, the immediate support of ISPs was needed.

Once [redacted] provided the IP address of the access point, RCMP could determine who the Internet Service Provider (ISP) was as certain blocks of IP addresses are issued to certain ISPs. This ISP information is openly available on the Internet. The ISP would subsequently be contacted and if they co-operated, they would give police the civic address. Police would then proceed to the area in an attempt to locate the suspect who would be operating within a quarter kilometer of the physical address of the access point.

However, without a warrant or court order, in this case the ISPs would not provide the customer name and address information to police. The most detailed information one ISP gave police was that the IP address was located somewhere on Yonge Street, which is a street that stretches from Lake Ontario to the city of Barrie.

Because of the lack of cooperation from ISPs it took eight full-time technical investigators five days to finally locate and arrest the suspects. The suspects' attempted frauds were valued at $100 million. They were successful at actually defrauding victims of $15 million.

The very fast moving nature of this investigation precluded investigators from obtaining warrants or court orders for the numerous IP addresses [redacted]

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

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

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

---

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

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

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 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. <u>Time delays, resource impacts, consequences for victims</u>

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

---

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

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

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' 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

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

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

---

Diego, California; 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.

[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.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

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

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

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***

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

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

Specific Examples from International Cases

2006-1251012
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.

2006-1035065
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).

2007-113950
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 2007-113950
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

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

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

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

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.

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.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

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)).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

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

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

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.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

CNA Consultations – Status and Planning Report

Groups	Method	Timing	Location
Federal Ombudsman for Victims of Crime **Steve Sullivan, Federal Ombudsman for Victims of Crime** **Louis Théorêt**	Meeting	Wednesday, Oct. 10th @ 1:00 – 2:15pm	269 Laurier 12th Floor, Section D BR D4700 (12ppl)
Canadian Resource Centre for Victims of Crime s.19(1) [redacted]	Meeting and possible written submission from NCECC	Wednesday, Oct. 10th @ 2:30 – 4:00pm	269 Laurier 17th Floor, Section B BR B2000 (16/34ppl)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

National Child Exploitation Coordination Centre (NCECC) **Earla-Kim McColl, Superintendent** **RCMP NCECC** **Susan Alter, RCMP Legal Counsel** [redacted]			
Ontario Provincial Police Child Pornography Section ("Project P") [redacted]	Conference Call	Thursday, Oct. 11th @ 1:00 – 2:30pm	269 Laurier 12th Floor, Section B BR B2600 (22ppl)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.19(1)

Geist – M
Yahoo!
CyberTip.ca

DRAFT 09-Oct-07

Office of Privacy Commissioner of Canada **Raymond D'Aoust, Assistant Privacy Commissioner** **+ 4 staff (policy, legal, etc.)**	Meeting	Monday, October 15th @ 2:00pm	269 Laurier 12th Floor, Section B BR B2600 (22 ppl)
[redacted] **International Perspectives**	Meeting and Written Submission	Thursday, Oct. 18th @ 2:00 – 3:30pm	269 Laurier 11th Floor, Section A BR A1600 (16ppl)
Yahoo! Canada [redacted]	Meeting	TBD	

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

DRAFT 09-Oct-07

Rogers Communications [redacted] **+ 2 additional staff (wireless, security)**	Meeting	Friday, Oct. 12th @ 10:00 – 11:30am	269 Laurier 13th Floor, Section D BR D4400 (20ppl)
Information Technology Association of Canada (ITAC) [redacted] **+ additional members** **Canadian Wireless Telecommunications Association (CWTA)** [redacted]	Meeting; CWTA also to provide written submission	Friday Oct. 12th @ 2:30 – 4:00pm	269 Laurier 12th Floor, Section B BR B2600 (22ppl)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Canadian Chamber of Commerce	Written Submission		
Canadian Internet Policy and Public Interest Clinic (CIPPIC) **Additional written comments from [redacted] Law, Ethics and Technology at the University of Ottawa**	Written Submission		
Still Awaiting Response: **B'nai Brith; Cybertip.ca**			

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

DRAFT 09-Oct-07

Canadian Association of Chiefs of Police (CACP) [redacted]	Written Submission; possible meeting (TBD)	TBD	
[redacted]	Written Submission (via media comments); possible meeting (TBD)	TBD Wed. 3pm	
[redacted]	Written Submission		

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Bell; Telus; Videotron **Canadian Association of Internet Providers (CAIP)** **Canadian Advanced Technology Alliance (CATA)** **IBM** **Canadian Bar Association** **Electro-Federation of Canada** s.19(1) [redacted] **Canadian Information Processing Society**			

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

SUMMARY OF PUBLIC CONSULTATION ON

ACCESS TO CUSTOMER NAME AND ADDRESS INFORMATION

FOR PUBLIC SAFETY PURPOSES

APRIL 2008

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

INTRODUCTION

Public Safety Canada, in collaboration with Industry Canada, undertook a public consultation on the subject of law enforcement and national security agencies' access to customer name and address information (CNA) in the possession of telecommunications service providers (TSPs) for public safety purposes. CNA information generally refers to basic identifiers such as a name, address, cell phone identifiers, Internet protocol (IP) and email addresses, or similar identifiers. The consultations were initiated in September 2007 and concluded in October 2007.

The purpose of the public consultation was to provide a range of stakeholders and the general public with an opportunity to express their current views and identify any new considerations with respect to this issue. Stakeholders were asked to consider a number of important factors, including: the challenges faced by law enforcement and national security agencies in the face of new technologies; the need to preserve and protect the privacy rights of all Canadians; and maintaining the competitiveness of the telecommunications sector.

A consultation document was posted on the Public Safety Canada website on September 12, 2007. The public was invited to provide input into the consultation process by October 12, 2007. Interested individuals and organizations from across Canada provided written comments by letter or through the Public Safety Canada consultation webpage. In addition, meetings and teleconferences were held with a number of groups and individuals. Those who participated in the consultation included representatives of law enforcement, victims groups, industry, civil liberties organizations, individuals and groups with an interest in privacy issues, and members of the general public.

SUMMARY

This summary is an overview of the comments and written submissions received from all groups and individuals who participated in the consultation process. The views and opinions of participants are presented below within one of five categories: law enforcement, victims groups, industry, privacy advocates, and public submissions. These categories are generally reflective of the orientation of participants, and are used to assist in presenting the views, opinions and information received.

LAW ENFORCEMENT

Law enforcement participants stressed the need for timely and consistent on-request access to CNA information for a variety of policing purposes, including the investigation of serious crimes such as child sexual exploitation, terrorism and other criminal activities. Participants were strongly of the view that legislation requiring the disclosure of CNA to law enforcement was essential for them to perform their duties effectively. Key features of any legislation would include clear obligations for TSPs and consistent practices with regard to the disclosure of CNA.

- Expressed concern over the lack of a clear legal framework governing TSP disclosure of CNA. Without clear obligations in the law, a variety of practices have developed among

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

TSPs with respect to the release of basic customer information. TSPs are deciding when to release CNA to police, under what circumstances, and with little consistency overall; thereby influencing the degree to which police are able to follow up on a potential lead, pursue an investigation, or rescue a victim from danger. If the TSP is not cooperative when a request for CNA is made, law enforcement agencies may have no means to compel the disclosure of this information.

- Expressed frustration over the increasing reluctance on the part of TSPs to assist police in accessing basic CNA information. This was linked to the area of child sexual abuse and exploitation, and was also flagged as a concern relevant to other investigations (especially on-line) and the pursuit of general policing duties.

- Noted that many TSPs do provide police with CNA information in child sexual abuse investigations, in part because they understand the seriousness of the crime, while also recognizing the unique challenges involved in fighting it. At the same time, according to the RCMP's National Child Exploitation Coordination Centre, on average one-third or about 35 percent of CNA information requests involving child sexual exploitation cases are denied, leaving many predators undetected and many children in abusive situations.

- Supported strong privacy safeguards as an important component of any legislative proposal providing for access to CNA upon request, but they did not consider judicial pre-authorization as an appropriate option (or even feasible in most instances). Emphasized that CNA is "pre-warrant" information that simply provides law enforcement with basic, non-sensitive identification information which carries little or no expectation of privacy. This information is often vital in early stages of investigations, and without which further investigation leading to a warrant may not be possible. Described CNA as telephone book information – with email and IP addresses analogous to traditional telephone identifiers, such as name, telephone and civic address.

- Described CNA information as a tool to investigate a lead and to help to confirm or remove people as potential suspects in a case. Emphasized that an investigation does not end with the acquisition of CNA information. Should law enforcement decide to pursue further investigatory measures that require prior judicial authorization, such as intercepting communications or searching a residence, police would seek an appropriate order from a court.

- Supported the use of administrative safeguards to ensure appropriate access to CNA information (in the context of a legislated obligation to provide the information on request); the safeguards could include limits on who can have access to the information and how it is used, as well as requirements for internal audits. Emphasized that lawful access to CNA does not include content of communications or website activity, and noted that police would clearly continue to obtain the necessary court orders to track web activity or to intercept private communications.

- Spoke to the favourable working relationships they have built over the years with established TSPs, for example the major phone companies, in requesting CNA in the course of their

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

duties. At the same time, pointed to the practical difficulties and burdens in trying to work with the over 400 Internet service providers (ISPs) that currently operate in the Canadian market.

- Expressed concern over the extremely high resource demands that would be placed on law enforcement organizations and the courts if police were required to seek judicial pre-authorization for all CNA inquiries.

- Noted that no law prohibits ISPs from informing a customer of police interest in their CNA information, and the related risk that ongoing criminal investigations can be compromised if such information is provided to the customer. Advised that some ISPs openly advertise their lack of cooperation with police to attract customers and hinder criminal investigations by informing customers that they will delete an account in the event of a "personal emergency".

- Emphasized that other countries, including the United Kingdom, Australia and the United States, do not require their law enforcement agencies to secure judicial pre-authorization to obtain CNA from a TSP, and that administrative safeguards appear to work well in those jurisdictions.

VICTIMS GROUPS

Victims groups shared many of the concerns and views expressed by law enforcement representatives. They strongly emphasized that access to CNA is first and foremost a public safety issue, and that the individual privacy rights of those who may be the subject of a criminal investigation do not, and should not, override the privacy rights of victims of crime - keeping in mind many victims are children who need to have police investigate crimes against them in order to protect their privacy (for example, where images of abuse are being displayed on the Internet). They highlighted that CNA is often crucial in the ability of law enforcement to rescue children from abusive situations and prosecute those responsible.

- Emphasized the difficulty for law enforcement in investigating child pornography and child luring cases without access to basic Internet identifiers such as IP and email addresses, noting that anonymity is inherent in many online communications.

- Expressed frustration over the lack of cooperation on the part of some TSPs to assist police by providing access to basic CNA information. Acute concern was expressed in the area of Internet-facilitated child sexual exploitation, while recognizing that CNA information may be important in other contexts as well.

- Victims groups shared the view of law enforcement that CNA was "pre-warrant" information that should not be subject to judicial pre-authorization. Stressed that the scope of CNA information accessible upon request should be well defined and recognized the need for strong safeguards to protect against possible abuses and ensure public confidence.

- Argued that TSPs have a responsibility for the environment that they create and profit from, and that part of that responsibility is to respond to law enforcement requests for assistance in

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

accessing CNA for public safety purposes. Expressed concerns that police are forced to rely on moral suasion, calls to abide by civic duty, and the goodwill of TSPs, when the lives of children and other victims hang in the balance.

- Noted that the Government of Canada signed the *Canadian Basic Statement of Principles for Victims of Crime* in 2003, which commits the federal, provincial and territorial governments to consider and respect the privacy of victims to the greatest extent possible and to take measures to protect victims. Noted that G-8 Ministers committed to ensuring the implementation and effectiveness of laws relating to child pornography.

- Recommended that the results of any audits of practices that might be required by new legislation should be provided to the Federal Ombudsman for Victims of Crime.

INDUSTRY

Industry - comprising telecommunications industry associations, individual TSPs, and other organizations with an interest in telecommunications - generally supported law enforcement and national security agencies' (LEAs) access to CNA for public safety purposes in appropriate circumstances. The main preoccupations for industry, should any new legislation come into place, were: to have clear and reasonable obligations in law; that companies receive reasonable compensation for costs incurred in providing CNA information; and, concern that new information collection, retention or verification obligations would not be created.

- Held that any new legislation or regulations must clearly outline TSP obligations, recognizing that many customers expect information to be protected and not disclosed. Rather than relying on discretion or judgement calls, they indicated a desire to see specifics regarding when, under what circumstances, and to whom to release CNA.

- If new legislation were to require on-request access to CNA by police and the Canadian Security and Intelligence Service (CSIS), strong administrative safeguards would be essential to protect the privacy interests of their customers. General acknowledgment that the privacy rights of individuals must be balanced with the requirements of law enforcement officials to track and prosecute criminals. Potential safeguards listed in the consultation document were seen as generally reasonable and rigorous.

- Some TSPs expressed a preference to continue to provide CNA only subject to a warrant or in exigent circumstances (i.e. imminent threat of harm to person or property). Where exigent circumstances or urgent need is demonstrated, many noted that they respond to LEAs as quickly and as diligently as possible. A number said that more clarity was needed to define the scope of exigent circumstances and when information must be provided.

- Some suggested it would be advantageous to look into alternative models, such as an expedited judicial authorization process (warrant or production order), or the creation of a lower threshold warrant for accessing CNA.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- Indicated that the scope of the CNA information listed in the consultation document extended beyond what might be commonly regarded by the general public as "basic customer information" (i.e. cell phone and Internet identifiers). Suggested that the types of "basic identifiers" sought for wireless and Internet services are more onerous to produce than those of traditional telecommunications services due to the sophistication of the technologies employed. As such, wireless and Internet providers felt they should not be compelled to provide greater levels of information than other TSPs operating traditional telecommunications technologies.

- Noted that traditional "tombstone data" such as customer name, civic address and telephone number information may be less privacy-sensitive than other types of identifiers. Underlined the importance of having customers understand there is a legal framework within which this information is provided to police.

- Recommended important safeguards with regard to designated officers, including a process in place to limit the number of contact points, ensure consistency, and validate the authority of the LEA officials requesting CNA. Some also suggested working with LEAs to create a standardized CNA request form to facilitate any request process.

- Suggested that provisions in any new legislation may need to deal differently with smaller and larger TSPs. New measures could have greater impacts and relative resource implications for smaller TSPs (e.g., any increase in requests for CNA may necessitate hiring and training more personnel, as well as upgrading or automating information systems).

- Expressed concern that the volume of requests for CNA could increase substantially under any new legislation if there were no judicial pre-authorization, with a corresponding and likely substantial increase in costs to TSPs.

- Noted that Canada's telecommunications industry has a long history of working cooperatively with law enforcement. Acknowledged that the ability to obtain CNA is an important tool for LEAs in their efforts to protect society, and underscored a desire to continue their positive relationships with law enforcement.

- Noted that large TSPs maintain dedicated security departments whose sole purpose is to respond to law enforcement requests and comply with court orders; that these services are provided in the interest of public safety by TSPs; and that there is an associated cost to providing this assistance, which is not insignificant.

PRIVACY ADVOCATES

Privacy stakeholders generally recognized that a lack of consistency with regard to CNA disclosure practices by TSPs represents a hindrance to law enforcement in their ability to pursue leads and investigate crimes. This lack of consistency alone, however, is not a sufficient justification for warrantless access to CNA, which most consider infringes upon civil liberties and individual privacy. The need for access to information must be demonstrated and concern was expressed that evidence to date is lacking. Above all, they stressed the importance of

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

appropriate oversight in the CNA disclosure process, with a very strong preference for judicial pre-authorization, to protect privacy and other rights under the *Canadian Charter of Rights and Freedoms*.

- Indicated that the law enforcement community should first clearly demonstrate the need for CNA, before the creation of a requirement for TSPs to provide this information on-request, is considered. Expressed the opinion that in the majority of cases police can obtain the information they need through traditional investigative means, including the use of a warrant or production order.

- The majority expressed that judicial pre-authorization should always be required for the release of any personal information to LEAs. Several suggested that the necessity for judicial pre-authorization may depend on the nature of the information being sought (e.g. warrants may not be necessary for information already in the public domain or for "tombstone data" including name, address, and telephone numbers). Some believed that options for access to CNA without judicial pre-authorization may be reasonable; however, most took the view that LEAs needed to do more to publicly demonstrate why there is a need to obtain it without judicial pre-authorization.

- Some contended that existing provisions within the *Criminal Code* and the *Personal Information Protection and Electronic Documents Act* (PIPEDA) provide the police with an adequate legislative framework and powers to investigate crimes, including Internet-related crime. They suggested that what is needed is more education and an effort to foster an enhanced cooperative working environment between TSPs and law enforcement.

- Some suggested examining mechanisms in the *Criminal Code* that either enable access to certain information at lower thresholds (i.e. the creation of a lower threshold warrant), or through the use of an expedited process for judicial authorization. Others felt that lowering the judicial threshold would be inappropriate given that personal information is involved. Opposition was also expressed by some to the idea of expediting CNA authorizations, suggesting that the *Criminal Code* already provides for an expedited process in which LEAs can access CNA in urgent situations – i.e. s.487.11 provides for warrantless searches in cases of exigent circumstances, including an urgent threat of serious harm to any person or property.

- Some felt that without judicial pre-authorization, the purposes for which law enforcement may demand CNA must be narrowly and precisely circumscribed (e.g. through a prescribed list of circumstances under which LEAs could obtain access to CNA upon request). Evidence would be required to justify the listing of circumstances in which warrantless, on-demand access to CNA would be appropriate.

- Shared industry's concern that the scope of the information listed in the consultation document extended beyond what might be appropriately regarded by members of the public as "basic customer information" (i.e. cell phone and Internet identifiers).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- Argued that although CNA pertains to seemingly innocuous personal identifiers, it has the potential to reveal sensitive personal information when combined with other information. For instance, separate pieces of information about an individual could potentially be combined so as to reveal more intimate personal information.

- Stressed the need for strong legislative safeguards to ensure the appropriate access to, use, and handling of CNA by LEAs. Concerned about the potential for abuse, such as the pursuit of "fishing expeditions" or the potential for LEAs to accumulate and retain large amounts of personal information on individuals. Pointed to the recent reported abuses and irregularities in the United States involving the use of administratively authorized search procedures. Some contributors suggested that the safeguards in the consultation document were insufficient in any context, and that additional safeguards should be in place even where judicial authorization is obtained.

- Indicated that a continuing review of any administrative model that might be created by statute (i.e., on-request access, with administrative safeguards) would be imperative. There would be a need to ensure that changes in technology and/or industry practices do not result in a process that violates the *Canadian Charter of Rights and Freedoms* by unduly infringing upon individuals' expectations of privacy.

- One participant suggested the creation of a working group in statute that would comprise government, industry, privacy and civil society representatives to provide ongoing advice on the administration of any legislation and review practices.

PUBLIC SUBMISSIONS

The majority of public submissions were opposed to law enforcement access to CNA information without judicial pre-authorization. Some mistakenly believed that judicial pre-authorization is required today in all cases. A perception was expressed by some that law enforcement may be attempting to extend its reach too far into the private lives of Canadians.

- Expressed strong opposition to law enforcement access to information in the online context. Many were mistakenly of the view that law enforcement and national security agencies were seeking unwarranted access to the content of communications, including email content and websites visited.

- Suggested that an absence of judicial pre-authorization creates the potential for abuses to occur through unnecessary access to personal information. Comparisons were made with recent reported abuses and irregularities in the United States.

- Expressed the view that there is a lack of publicly available evidence clearly demonstrating law enforcements' need to access CNA without judicial pre-authorization.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

PUBLIC CONSULTATIONS ON

ACCESS TO CUSTOMER NAME AND ADDRESS INFORMATION (CNA)

FOR PUBLIC SAFETY PURPOSES

SUMMARY OF CONSULTATION INPUT

DECEMBER 2007

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

INTRODUCTION

Public Safety Canada, in collaboration with Industry Canada, undertook a public consultation on the subject of lawful access to customer name and address information (CNA) in the possession of telecommunications service providers (TSPs) by law enforcement and national security agencies. The consultations were initiated in early September 2007 and concluded in mid October 2007. This subject was previously considered by stakeholders in public consultation processes on lawful access issues that were held in 2002 and 2005.

The provision of personal information to law enforcement and national security agencies by telecommunications service providers is not currently governed by any specific legislation. As such, a range of practices exists today - some service providers will provide requested information in many or most circumstances; others will do so only in certain limited cases; and others will refuse to do so without judicial authorization, regardless of the circumstances. The context in which the issue of access to customer information must be considered is both national and international. The matters that public safety and national security agencies are charged with addressing – from returning stolen property, to combating frauds, child pornography and the threat of terrorism - can be complex and will regularly cross borders. Fast paced changes in technology and the telecommunications marketplace create further challenges from public safety, industry competitiveness and personal privacy points of view.

The purpose of the consultations was to obtain current views and identify any new considerations in respect of possible approaches in this area. Stakeholders were asked to consider a number of important factors, including: the challenges faced by law enforcement and national security agencies in the face of new technologies; the need to preserve and protect the privacy rights of all Canadians; maintaining the competitiveness of the telecommunications sector; and ensuring that an unreasonable burden is not placed on the Canadian public.

A consultation document was posted to the Public Safety Canada website on September 12, 2007 (**Annex A**), with an invitation to the public to provide input into the consultation process by October 12, 2007. Interested individuals and organizations from across Canada provided written comments by letter or through the Public Safety Canada consultation webpage. In addition, a number of meetings and teleconferences were held with selected groups and individuals. Stakeholders who provided input into the consultations included representatives of law enforcement, victims' groups, industry, civil liberties organizations, individuals and groups with an interest in privacy issues, and the general public.

SUMMARY OF CONSULTATION INPUT

This summary is an overview of the comments and written submissions received from all groups and individuals who provided input. The input is presented below within one of five categories: law enforcement, victims' groups, industry, privacy advocates, and public submissions. These categories are generally reflective of the orientation of participants, and are used to assist in presenting the available information. Any input received that touched upon issues beyond the scope of the CNA information issue is not reflected in the summary.

000048

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

LAW ENFORCEMENT

Law enforcement participants stressed the need for timely and consistent on-request access to CNA information for a variety of policing purposes, including the investigation of serious crimes such as child sexual exploitation, terrorism and other criminal activities. Participants were strongly of the view that legislation requiring the disclosure of CNA to law enforcement was essential for them to perform their duties effectively. Key features of any legislation would include clear obligations for TSPs and consistent practices with regard to the disclosure of CNA.

- Recognized that strong privacy safeguards are an important component of any legislative scheme providing for access to CNA upon request, but they did not consider judicial pre-authorization as an appropriate option (or even feasible in certain circumstances). Emphasized that CNA is "pre-warrant" information that simply provides law enforcement with basic, non-sensitive identification information which carries little or no expectation of privacy. This information is often vital in early stages of investigations, and without which further investigation leading to a warrant may not be possible. Described CNA as telephone book information – with Email and IP addresses analogous to traditional telephone identifiers, such as name, telephone and civic address.

- Supported the use of administrative safeguards to ensure appropriate access to CNA information (in the context of a legislated obligation to provide the information on request); the safeguards could include limits on who can have access to the information and how it is used, as well as requirements for internal audits. Emphasized that lawful access to CNA does not include content of communications or website activity, unless a court order or warrant is issued.

- Emphasized that other countries, including the United Kingdom, Australia and the United States, do not require their law enforcement agencies to secure judicial authorization to obtain CNA from a TSP, and that administrative safeguards appear to work well in those jurisdictions.

- Described CNA information as a tool to investigate a lead and to confirm or remove people as potential suspects in a case. Emphasized that an investigation does not end with the acquisition of CNA information. Should law enforcement decide to pursue further investigatory measures, such as intercepting communications or searching a residence, a warrant would always be required.

- Noted that judicial oversight in criminal proceedings already exists and that this oversight can include a review of the collection and use of CNA by a court, where relevant.

- Expressed concern over the extremely high resource demands that would be placed on law enforcement organizations and the courts if police were required to seek judicial authorization for all CNA inquiries.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- Expressed frustration over the increasing reluctance on the part of TSPs to assist police in accessing basic CNA information. This was linked principally to the area of child sexual abuse and exploitation, and was also flagged as a concern relevant to national security investigations, other criminal activity (especially on-line) and the pursuit of general policing duties.

- Expressed concern over the lack of clear obligations in law governing TSP disclosure of CNA. TSPs are deciding when to release CNA to police, under what circumstances, and with little consistency overall; thereby influencing the degree to which police are able to follow up on a potential lead, pursue an investigation, or rescue a victim from danger.

- Spoke to the favourable working relationships they have built over the years with TSPs in requesting CNA in the course of their duties. At the same time, pointed to the practical difficulties and burdens in trying to work with the over 400 Internet service providers (ISPs) that currently operate in the Canadian market.

- Noted that no law prohibits ISPs from informing a subscriber of police interest in their CNA information and the related risk that ongoing criminal investigations can be compromised. Advised that some ISPs cater to criminal activity online, including sheltering child pornography and offering to immediately erase illegal content upon a subscriber's request.

- Noted that many TSPs do provide police with CNA information in child sexual abuse investigations, in part because they understand the seriousness of the crime, while also recognizing the unique challenges involved in fighting it. However, according to the RCMP's National Child Exploitation Coordination Centre (NCECC), 30-40 percent of CNA information requests involving child sexual exploitation are denied, leaving many predators undetected and many children in abusive situations.

VICTIMS' GROUPS

Victims' groups shared many of the concerns and views expressed by law enforcement representatives. They strongly emphasized that access to CNA is first and foremost a public safety issue, and that individual privacy does not, and should not, override the privacy rights of victims of crime and children. They highlighted that CNA is often crucial in the ability of law enforcement to rescue children from abusive situations and prosecute those responsible.

- Emphasized the difficulty for law enforcement in investigating child pornography and child luring cases without access to basic Internet identifiers such as IP and Email addresses, noting that anonymity is inherent in many online communications.

- Victims' groups shared the view of law enforcement that CNA was "pre-warrant" information that should not be subject to judicial pre-authorization. Stressed that the scope of CNA information accessible upon request should be well defined and recognized the need for strong safeguards to protect against possible abuses and ensure public confidence.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- Noted that the Government of Canada signed the *Canadian Basic Statement of Principles for Victims of Crime* in 2003, which commits the federal government to consider and respect the privacy of victims to the greatest extent possible and to take measures to protect victims. Noted that G-8 Ministers committed to ensuring the implementation and effectiveness of laws relating to child pornography.

- Expressed frustration over the lack of cooperation on the part of some TSPs to assist police in accessing basic CNA information. Acute concern was expressed in the area of Internet-facilitated child sexual exploitation, while recognizing that CNA information may be important in other contexts as well.

- Argued that TSPs have a responsibility for the environment that they create and profit from, and that part of that responsibility is to respond to law enforcement requests for assistance in accessing CNA for public safety purposes. Expressed concerns that police are forced to rely on moral suasion, calls to abide by civic duty, and the goodwill of TSPs, when the lives of children and other victims hang in the balance.

- Recommended that the results of any audits of practices that might be required by new legislation should be provided to the Federal Ombudsman for Victims of Crime.

INDUSTRY

Industry - comprising telecommunications industry associations, TSPs, and other organizations with an interest in telecommunications - generally supported the principle of law enforcement and national security agencies' (LEAs) access to CNA for public safety purposes in appropriate circumstances. The main preoccupations for industry, should any new legislation come into place, were: to have clear and reasonable obligations in law; that companies receive reasonable compensation for costs incurred in providing CNA information; and, ensuring that new information collection, retention or other additional obligations would not be created.

- Noted that Canada's telecommunications industry has a long history of working cooperatively with law enforcement. Acknowledged that the ability to obtain CNA is an important tool for LEAs in their efforts to protect society, and underscored a desire to continue their positive relationships with law enforcement.

- Noted that large TSPs maintain dedicated security departments whose sole purpose is to respond to law enforcement requests and comply with court orders, and that these services are provided at considerable cost to TSPs.

- Held that any new legislation or regulations must clearly outline TSP obligations, recognizing that many customers expect information to be protected and not disclosed. Rather than relying on discretion or judgement calls, they indicated a desire to see specifics regarding when, under what circumstances, and to whom to release CNA.

- Suggested that provisions in any new legislation may need to deal differently with smaller and larger TSPs. New measures could have greater impacts and relative resource implications for

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

smaller TSPs (e.g., any increase in requests for CNA may necessitate hiring and training more personnel, as well as upgrading or automating information systems).

- Some TSPs expressed a preference to continue to provide CNA only subject to a warrant or in exigent circumstances (i.e. imminent threat of harm to person or property). Where exigent circumstances or urgent need is demonstrated, many noted that they respond to LEAs as quickly and as diligently as possible. A number said that more clarity was needed to define the scope of exigent circumstances.

- Suggested it would be advantageous to look into alternative models, such as an expedited judicial oversight (warrant or production order) process, or the creation of a lower threshold warrant for accessing CNA.

- Expressed concern that the volume of requests for CNA could increase substantially under any new legislation if there were no judicial oversight, with a corresponding and likely substantial increase in costs to TSPs.

- Indicated that the scope of the information listed in the consultation document extended beyond what might be commonly regarded by members of the public as "basic customer information" (e.g. cell phone identifiers, Email and IP address). Noted that customer name, civic address and telephone number information may be less sensitive than these other kinds of identifiers, in terms of providing access to police.

- If new legislation were to require on-request access to CNA by police and CSIS, strong administrative safeguards would be essential to protect the privacy interests of their subscribers. Most generally acknowledged that the privacy rights of individuals must be balanced with the requirements of law enforcement officials to track and prosecute criminals. Potential safeguards listed in the consultation document were seen as generally reasonable and rigorous.

- Recommended important safeguards with regard to designated officers, including a process in place to limit the number of contact points, ensure consistency, and validate the authority of the LEA officials requesting CNA. Some also suggested working with LEAs to create a standardized CNA request form to facilitate the request process.

PRIVACY ADVOCATES

Privacy stakeholders generally recognized that a lack of consistency with regard to CNA disclosure practices by TSPs represents a hindrance to law enforcement. This lack of consistency alone, however, is not a sufficient justification for infringing upon civil liberties and individual privacy through warrantless access to CNA. The need for access to information must be demonstrated and evidence to date is lacking. Above all, they stressed the importance of appropriate judicial oversight in the CNA disclosure process to protect privacy and other rights under the *Charter of Rights and Freedoms*.

000052

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- Indicated that the law enforcement community must first clearly demonstrate the need for CNA, before considering a requirement for TSPs to provide this information on-request. Believed that in the majority of cases police can obtain the information they need through traditional investigative means, including the use of a warrant or production order.

- Concerned about the potential for abuse of legislated on-request access to CNA by law enforcement, such as the pursuit of "fishing expeditions" or the potential for LEAs to accumulate and retain large amounts of personal information on individuals.

- Argued that although CNA pertains to seemingly innocuous personal identifiers, it has the potential to reveal sensitive personal information when combined with other information. For instance, each separate piece of information about an individual, when added up, could potentially reveal intimate personal details about the person.

- Shared industry's concern that the scope of the information listed in the consultation document extended beyond what might be appropriately regarded by members of the public as "basic customer information" (e.g. cell phone identifiers, Email and IP address).

- The majority expressed that judicial pre-authorization should always be required for the release of any personal information to LEAs. Several suggested that the necessity for judicial pre-authorization may depend on the nature of the information being sought (e.g. warrants may not be necessary for information already in the public domain; tombstone data including name, address, and telephone numbers). Some believed that options for access to CNA without judicial authorization may be reasonable, but only if LEAs publicly demonstrated specifically why there is a need to obtain it without judicial authorization.

- Some contended that existing provisions within the *Criminal Code* and the *Personal Information Protection and Electronic Documents Act* (PIPEDA) provide the police with an adequate legislative framework and powers to investigate crimes, including Internet-related crime. They suggested that what is needed is more education and an effort to foster an enhanced cooperative working environment between TSPs and law enforcement.

- Some suggested examining mechanisms in the *Criminal Code* that either enable access to certain information at lower thresholds (i.e. the creation of a lower threshold warrant), or through the use of an expedited process for judicial authorization. Others felt that lowering the judicial threshold would be inappropriate given that personal information is involved. Opposition was also expressed by some to the idea of expediting CNA authorizations, suggesting that the *Criminal Code* already provides for an expedited process in which LEAs can access CNA in urgent situations – i.e. s.487.11 provides for warrantless searches in cases of exigent circumstances, including an urgent threat of serious harm to any person or property.

- Some felt that without judicial pre-authorization, the purposes for which law enforcement may demand CNA must be narrowly and precisely circumscribed (e.g. through a prescribed list of circumstances under which LEAs could obtain access to CNA upon request). Evidence

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

would be required to justify the listing of circumstances in which warrantless, on-demand access, to CNA would be appropriate.

- Indicated that a continuing review of any administrative model that might be created by statute (i.e., on-request access, with administrative safeguards) would be imperative. There would be a need to ensure that changes in technology and practice did not result in a process that violates the *Canadian Charter of Rights and Freedoms* by unduly infringing upon individuals' expectations of privacy.

- Stressed the need for strong legislative safeguards to ensure the appropriate access, use and handling of CNA by LEAs. Pointed to the recent abuses and irregularities uncovered in the United States involving the use of administratively authorized search procedures contained in the *Patriot Act* as evidence of the potential for abuse. Some contributors suggested that the safeguards in the consultation document were inadequate from a privacy perspective.

- One participant suggested the creation of a working group in statute that would comprise government, industry, privacy and civil society representatives to provide ongoing advice on the administration of any legislation and review practices.

PUBLIC SUBMISSIONS

The majority of public submissions took a firm stance against law enforcement access to CNA information without judicial pre-authorization. Many mistakenly believed that judicial authorization is required today in all cases. A general perception was expressed that law enforcement may be attempting to extend its reach too far into the private lives of Canadians.

- Expressed strong opposition to law enforcement access to information in the online context. Many were mistakenly of the view that law enforcement and national security agencies were seeking unwarranted access to the content of communications, including email content and websites visited.

- Suggested that an absence of judicial pre-authorization creates the potential for abuses to occur through unnecessary access to personal information. Comparisons were made with recent reported abuses and irregularities in the United States.

- Pointed to a lack of publicly available evidence clearly demonstrating law enforcements' need to access CNA without judicial pre-authorization.

000054

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Blain, Christopher

From: Tait, Amanda [Amanda.Tait@ps-sp.gc.ca]

Sent: October 16, 2007 3:24 PM

To: LePage, Louis: DIF; Leduc, Andre: ECOM; Noir, Charles: ECOM; Conrad, Alexis: DBR; stinsond@smtp.gc.ca; kirkg@smtp.gc.ca; Lori Swift; Blain, Christopher; Audcent, Karen; Tom Konarski; Woodcock, Christopher

Cc: Deacon, James; Touizrar, Yacine; Cherian, Jovita; Auger, Julie

Subject: Updated CNA Consultation Schedule

Attachments: Consultation Timeline 16-10-07.doc

Hi all,

Please find attached an updated consult schedule. For quick reference, we only have two more meetings planned:

1) Wednesday, Oct. 17th 3:00-4:00pm with Michael Geist (269 Laurier, 16th Floor, Section B, BR 4200)

2) Thursday, Oct. 18th 2:00-3:30pm with [redacted] (269 Laurier, 11th Floor, Section A, BR A1600)

FYI – For those interested, I've attached links to articles written by [redacted] on Lawful Access (http://www.intergovworld.com/article/009bd5470a01040801683e80a42c6f6e/pg1.htm) (http://www.intergovworld.com/article/fbc625010a01040801fdf17cbf0f5f7e/pg1.htm) – may be helpful to read before we meet with her.

I haven't yet received a response from Yahoo Canada or Cybertip.ca (both of whom previously indicated a desire to meet). I'm taking this to mean that they are no longer interested in meeting for whatever reason. Will update if I hear otherwise.

As usual, please let me know if you are planning on attending so I can provide your name to security.

Cheers,

Amanda Tait
Policy Analyst /Analyste politique
Investigative and Telecommunication Technologies Policy/ Politiques des technologies d'investigation et de télécommunication
National Security Policy Division/ Direction générale des politiques de la sécurité nationale
Public Safety Canada/ Sécurité publique Canada
Tel/Tél: (613) 949-3184
E-mail/Courriel: Amanda.Tait@ps-sp.gc.ca

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Blain, Christopher

From: Tait, Amanda [Amanda.Tait@ps-sp.gc.ca]

Sent: October 9, 2007 4:05 PM

To: Conrad, Alexis: DBR; Leduc.Andre@ic.gc.ca; Noir, Charles: ECOM; stinsond@smtp.gc.ca; kirkg@smtp.gc.ca; Lori Swift; Blain, Christopher; Angers, Lucie; Tom Konarski; LePage, Louis: DIF; Bilodeau, Richard: #CB - BC

Cc: Deacon, James; Touizrar, Yacine; Auger, Julie; Cherian, Jovita; Rousseau, Chantale

Subject: Revised Consultation Schedule

Importance: High

Attachments: Consultation Timeline 09-10-07.doc

Hi all,

Attached is the most up-to-date version of the consultation schedule. Please note that the location of the meetings has changed – larger boardrooms were required due to level of participation.

Please plan to arrive **15 minutes prior** to the scheduled start time – this will give us a chance to discuss briefly before each meeting and will ensure that everyone is present before the arrival of the stakeholders.

There will be someone downstairs in the lobby to escort you to the appropriate boardroom. If necessary, please contact Chantale Rousseau at 613- 998-7482 and she will send someone to sign you in.

Cheers,

Amanda Tait
Policy Analyst /Analyste politique
Investigative and Telecommunication Technologies Policy/ Politiques des technologies d'investigation et de télécommunication
National Security Policy Division/ Direction générale des politiques de la sécurité nationale
Public Safety Canada/ Sécurité publique Canada
Tel/Tél: (613) 949-3184
E-mail/Courriel: Amanda.Tait@ps-sp.gc.ca

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Blain, Christopher

Subject: Updated: CNA Consultations
Location: 269 Laurier Ave. West, 16th floor, boardroom 16B 4200

Start: Fri 05/10/2007 1:00 PM
End: Fri 05/10/2007 2:00 PM

Recurrence: (none)

Meeting Status: Accepted

Meeting is to discuss CNA consultations
Date and Time: Friday, October 5th, 1:00-2:00pm
Location: 269 Laurier, 16th floor section B, boardroom 16B 4200

Agenda:

1) Status report;

2) Review consultation schedule and participation of depts/agencies - document to be distributed; and

3) Lawful Access legislation next steps.

A draft schedule will be sent out by COB today. A number of stakeholders have yet to respond with availability - schedule will be updated as responses come in.

Thank -you,

Amanda Tait
Policy Analyst /Analyste politique
Investigative and Telecommunication Technologies Policy/ Politiques des technologies d'investigation et de télécommunication

National Security Policy Division/ Direction générale des politiques de la sécurité nationale
Public Safety Canada/ Sécurité publique Canada
Tel/Tél: (613) 949-3184
E-mail/Courriel: Amanda.Tait@ps-sp.gc.ca

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Consultations on Customer Name and Address Information

Purpose:

- Obtain views from stakeholders on the issue of law enforcement and CSIS access to basic customer information to undertake their duties. This is not a consultation on specific proposals, but rather on possible approaches and any key concerns or considerations relevant to this issue from stakeholder points of view.

Format:

- Officials are in listening mode, seeking views and perspectives and any information stakeholders deem relevant to the issue of access to basic customer information. Officials may ask questions of stakeholders on various facets of the issue.

- There is no mandate for officials to consult on other issues at this time, but stakeholder views on how other issues may have an impact on the question of access to basic customer information are most welcome, should stakeholders see this as valuable.

- A brief introduction on the purpose and format will be provided by PS for each meeting or teleconference. Formal introductions of those present, on both sides of the table, will follow.

- Stakeholders will be advised that notes are being taken, but that no tape recording is being made. They will be advised that should access to information requests be made, all notes may be subject to review and disclosure under access and privacy legislation.

- Stakeholders will be reminded that written submissions are welcome, and that submissions as soon as possible would be appreciated - given that October 12 was the original deadline for the consultations process.

Participation:

A) Stakeholder groups (as will be decided by those groups - no limits placed on numbers participating at this time)

B) Officials: PS (hosting) and IC and .....**TBC**?.

C) Ministers' offices: Representatives from the offices of the Ministers of Public Safety and Industry to attend as observers.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

CUSTOMER NAME AND ADDRESS (CNA) INFORMATION CONSULTATION DOCUMENT

INTRODUCTION

Modern telecommunications and computer networks such as the Internet are a great source of economic and social benefits, but they can also be used in the planning, coordination, financing and perpetration of crimes and threats to public safety and the national security of Canada. By extension, the rapidly evolving nature of these technologies can pose a significant challenge to law enforcement and national security officials who are entrusted with combating these threats, and who employ lawful access to communications and information to do so.

The principles and powers of lawful access must be exercised in a manner consistent with the rights and freedoms guaranteed in the *Canadian Charter of Rights and Freedoms* and while adapting to the rapid pace of technological change.

THE CONSULTATION PROCESS

Public Safety Canada, in collaboration with Industry Canada, is presently examining how to address the challenges faced by police, the Canadian Security Intelligence Service (CSIS) and the Competition Bureau when seeking timely access to basic CNA information in a modern telecommunications milieu. This question was previously considered by stakeholders in broader consultation processes on lawful access issues held in 2002 and 2005.

The purpose of this consultation is to provide a range of stakeholders - including police and industry representatives and groups interested in privacy and victims of crime issues - with an opportunity to identify their current views on possible approaches to updating Canada's lawful access provisions as they relate to law enforcement and national security officials' need to gain access to CNA information in the course of their duties. The possible scope of CNA information to be obtained is later identified, but it should be noted from the outset that it would not, in any formulation, include the content of communications or the Web sites an individual visited while online.

The objectives of this process are to maintain lawful access for law enforcement and national security agencies in the face of new technologies while preserving and protecting the privacy and other rights and freedoms of all people in Canada. In striving to attain these goals, it is essential to ensure that the competitiveness of Canadian industry is taken into account and that the solutions adopted do not place an unreasonable burden on the Canadian public.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

CURRENT CONTEXT

Timely access to CNA information is an important tool used by law enforcement and national security agencies to fulfil their public safety mandates. This type of information can be vital in the context of investigations of online criminal activity, such as child exploitation.

Law enforcement agencies have been experiencing difficulties in consistently obtaining basic CNA information from telecommunications service providers (TSPs). In the absence of explicit legislation, a variety of practices exists among TSPs with respect to the release of basic customer information, e.g., name, address, telephone number, or their Internet equivalents. Some companies provide this information voluntarily, while others require a warrant before providing any information, regardless of its nature or the nature of the situation. If the custodian of the information is not cooperative when a request for such information is made, law enforcement agencies may have no means to compel the production of information pertaining to the customer. This poses a problem in some contexts. For example, law enforcement agencies may require the information for non-investigatory purposes (e.g., to locate next-of-kin in emergency situations) or because they are at the early stages of an investigation. The availability of such building-block information is often the difference between the start and finish of an investigation.

CNA INFORMATION

In the context of options under consideration by Public Safety Canada and its partner departments and agencies, CNA information refers to basic identifiers that would assist law enforcement and national security agencies to determine the identity of a telecommunications service subscriber, if this information was necessary to the performance of their duties.

The scope of CNA information obtained could include the following basic identifiers associated with a particular subscriber:

- name;
- address(es);
- ten-digit telephone numbers (wireline and wireless);
- Cell phone identifiers, e.g., one or more of several unique identifiers associated with a subscriber to a particular telecommunications service (mobile identification number or MIN; electronic serial number or ESN; international mobile equipment or IMEI number; international mobile subscriber identity or IMSI number; subscriber identity module card number of SIM Card Number);
- e-mail address(es);

000060

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- IP address; and/or,

- Local Service Provider Identifier, i.e., identification of the TSP that owns the telephone number or IP address used by a specific customer.

POSSIBLE MODEL

Options based on an administrative model are being considered closely by officials.

POSSIBLE SAFEGUARDS

Further to input received during 2002 and 2005 consultations, a number of safeguards could be included under a possible administrative model requiring the release of limited basic CNA information to law enforcement and national security agencies upon request. These could include:

- clear limitations on what customer information could be obtained upon request;

- limiting the number of employees who would have access to CNA;

- requiring that individuals with access be designated by senior officials within their organizations;

- limiting requests to those made for the purpose of performing an official duty or function;

- requiring that requests be made in writing, except in exceptional circumstances;

- requiring that designated officials provide associated information with their request, e.g., identification of a specific date and time for a request relating to an IP address;

- requiring designated officials to record their status as such when making a request, as well as the duty or function for which a particular request is made;

- limiting the use of any information obtained to the agency that obtained it for the purpose for which the information was obtained, or for a use consistent with that purpose, unless permission is granted by the individual to whom it relates;

- requiring regular internal audits by agency heads to ensure that any requests for CNA information are being made in accordance with the protocols and safeguards in place;

- reporting to responsible ministers on the result of any internal audits;

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- provision of any audit results to the Privacy Commissioner of Canada, the Security Intelligence Review Committee, or provincial privacy commissioners, as appropriate; or

- provision for the Privacy Commissioner and SIRC to conduct audits related to the release of CNA information.

Under no option being examined would TSPs be compelled to track the actions of customers or to collect information about them in the absence of necessary court authorizations governing such activity in Canada, nor would law enforcement or national security agencies be permitted to obtain the content of a customer's communications without such authorizations.

CONCLUSION

Officials plan to meet with a range of interested parties in September, 2007 to discuss the issues raised in this paper.

Written comments may also be sent to the following address by September 25, 2007, and will be gratefully received:

Customer Name and Address Consultation
Public Safety Canada
16C, 269 Laurier Avenue West
Ottawa, ON, Canada K1A 0P8

000062

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

XXX
XXXX
XXXXX

Dear XXX:

Public Safety Canada will be seeking your input over the next several weeks regarding possible measures to address law enforcement and national security agencies' lawful access requirements as they pertain to customer name and address information held by telecommunications service providers.

Please find attached for your consideration the consultation document that will serve as the basis for discussions. Lawful access has been the subject of two previous rounds of stakeholder consultations in 2002 and 2005. As suggested in the attached document, the upcoming consultation process will exclusively address possible approaches for law enforcement and national security agencies to gain necessary access to customer name and address information, while ensuring appropriate safeguards for the protection of privacy.

Your input on any or all of the issues identified in the consultation document is welcomed. A series of in-person meetings in Ottawa or teleconferences are being arranged to begin shortly. Alternatively, you may wish to submit input in writing to the address included in the attached document. If you choose to do so, please provide your written comments by September 25, 2007.

Should you have an interest in participating in the consultations, I would ask that you please contact Ms. Amanda Tait, Policy Officer, at 613 949-3184 or Amanda.tait@ps.gc.ca, for additional details and to arrange your participation.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

I thank you for your interest in this important public safety issue and look forward to receiving your comments.

Sincerely,

Lynda Clairmont
Associate ADM

/

J. Scott Broughton
Senior ADM

Emergency Management and National Security

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Date: September 10, 2007
Classification: Unclassified
Agency: Public Safety Canada

QP Note

STAKEHOLDER CONSULTATIONS ON CNA INFORMATION

ISSUE:

Anticipated questions concerning consultations with select stakeholders on the question of police and CSIS access to customer name and address information held by telecommunication service providers.

PROPOSED RESPONSE:

- **The purpose of the consultations is to provide a range of stakeholders - including the police, industry representatives, and groups interested in privacy and victims of crime issues - with an opportunity to identify their current views.**

- **Police can use this limited information to help investigate crimes, such as child pornography or luring over the Internet.**

- **A balance is needed to ensure public safety while respecting Canadians' right to privacy.**

If pressed on the kinds of information under discussion

- **Customer name and address information held by service providers can include a telephone number, and e-mail and Internet Protocol addresses.**

- **This is <u>not</u> information about which telephone numbers a customer has called, which websites a customer has visited, or the content of any communications. Access to those kinds of information require court authorization, such as a warrant.**

Deleted: the

<u>Description of Issue</u>:

Possible media attention on the consultations, with a particular focus on privacy concerns.

<u>Background:</u>

Public Safety Canada, in collaboration with Industry Canada, is presently examining how to address the challenges faced by police, the Canadian Security Intelligence Service (CSIS) and the Competition Bureau when seeking timely access to basic CNA information in the modern telecommunications environment. The September 2007 consultations will represent the third round of stakeholder consultations on access to CNA information (broad consultations on lawful access took place in 2002 and 2005).

The purpose of the 2007 round of consultations is to provide a range of select stakeholders - including the police, industry representatives and groups interested in privacy and victims of crime issues - with an opportunity to identify their current views on possible approaches to updating Canada's lawful access provisions as they relate to law enforcement and national security officials' need to gain access to CNA information in the course of their duties.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

CNA information refers to basic customer identifiers (e.g. name, address, telephone number, Internet Protocol (IP) address, e-mail address, and cell phone identifiers) that can help law enforcement and CSIS determine the address or identity of a suspect, target or victim. Timely access to basic CNA information is an important tool used by law enforcement and national security agencies to fulfil their public safety mandates. This type of information can be vital in the context of investigations of online criminal activity, such as child exploitation.

Law enforcement agencies have been experiencing difficulties in consistently obtaining basic CNA information from telecommunications service providers (TSPs). In the absence of explicit legislation, a variety of practices exists among TSPs with respect to the release of basic customer information. Some companies provide this information voluntarily, while others require a warrant before providing any information, regardless of its nature or the nature of the situation. If the custodian of the information is not cooperative when a request for such information is made, law enforcement agencies may have no means to compel the production of information pertaining to the customer. This poses a problem in some contexts. For example, law enforcement agencies may require the information for non-investigatory purposes (e.g., to locate next-of-kin in emergency situations) or because they are at the early stages of an investigation. The availability of such building-block information is often the difference between the start and finish of an investigation.

Further to input received during 2002 and 2005 consultations, a number of safeguards are being considered under a possible administrative model requiring the release of limited basic CNA information to law enforcement and national security agencies upon request (e.g. limiting the scope and type of information obtained; limiting the number of persons authorized to request the information; and providing for numerous reporting and auditing requirements).

Under no option being examined would TSPs be compelled to track the actions of customers or to collect information about them in the absence of necessary court authorizations governing such activity in Canada, nor would law enforcement or national security agencies be permitted to obtain the content of a customer's communications without such authorizations.

CONTACTS:			
Prepared by	Tel. no.	Approved by (one name only)	Tel. no.
Amanda Tait	949 3184		

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

DRAFT 05-Oct-07

CNA Consultations – Status and Planning Report

Groups	Method	Timing	Location
Federal Ombudsman for Victims of Crime **Steve Sullivan, Federal Ombudsman for Victims of Crime** **+ additional staff**	Meeting	Wednesday, Oct. 10th @ 1:00pm	269 Laurier 11th Floor, Section D BR 4600
Canadian Resource Centre for Victims of Crime [redacted] **National Child Exploitation Coordination Centre**	Meeting and possible written submission from NCECC	Wednesday, Oct. 10th @ 2:30 pm	269 Laurier 11th Floor, Section D BR 4600

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

DRAFT 05-Oct-07

(NCECC) **Earla-Kim McColl** **+ additional staff**			
Ontario Provincial Police Child Pornography Section ("Project P") [redacted]	Conference Call	Thursday, Oct. 11th @ 1:00 pm	269 Laurier 16th Floor, Section B BR 4200

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Information Technology Association of Canada (ITAC) [redacted] **+ additional members**	Meeting	TBD - morning of Thurs. Oct. 11th or afternoon of Friday Oct. 12th	TBD
Rogers Communications [redacted] **+ additional staff**	Meeting	Friday, Oct. 12th @ 10:00am	TBD

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

DRAFT 05-Oct-07

Office of Privacy Commissioner of Canada **Raymond D'Aoust, Assistant Privacy Commissioner** **+ 4 staff (policy, legal, etc.)**	Meeting	Monday, October 15th, @ 2:00 pm	269 Laurier 12th Floor, Section B BR 2600
[redacted] **International Perspectives**	Meeting and Written Submission	Thursday, Oct. 18th @ 2:00pm	269 Laurier 16th Floor, Section B BR 4200
Yahoo! Canada [redacted] **+ additional staff**	Meeting	TBD	

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Canadian Association of Chiefs of Police (CACP) [redacted]	Written Submission; possible meeting (TBD)	TBD	
	Written Submission (via media comments); possible meeting (TBD)	TBD	

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

[redacted]	Written Submission via email		
Still Awaiting Response: **B'nai Brith; Cybertip.ca** **Bell; Telus** **Canadian Association of Internet Providers (CAIP)** **Canadian Wireless Telecommunications Association (CWTA)** **IBM** **Canadian Bar Association**			

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

DRAFT 05-Oct-07

Canadian Information Processing Society			

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

CNA Consultations – Status and Planning Report

Groups	Method	Timing	Location
Federal Ombudsman for Victims of Crime **Steve Sullivan, Federal Ombudsman for Victims of Crime** **+ additional staff**	Meeting	Wednesday, Oct. 10th @ 1:00pm	269 Laurier 11th Floor, Section D BR 4600
Canadian Resource Centre for Victims of Crime [redacted]	Meeting	Wednesday, Oct. 10th @ 2:30 pm	269 Laurier 11th Floor, Section D BR 4600

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Ontario Provincial Police Child Pornography Section ("Project P") [redacted]	Conference Call	Thursday, Oct. 11th @ 1:00 pm	269 Laurier 16th Floor, Section B BR 4200
Information Technology Association of Canada (ITAC) [redacted] **+ additional members**	Meeting	TBD - morning of Thurs. Oct. 11th or afternoon of Friday Oct. 12th	TBD

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Rogers Communications [redacted] **+ additional staff**	Meeting	TBD – week of Oct. 8th	TBD
Office of Privacy Commissioner of Canada **Raymond D'Aoust, Assistant Privacy Commissioner** **+ 4 staff (policy, legal, etc.)**	Meeting	Monday, October 15th, @ 2:00 pm	269 Laurier 12th Floor, Section B BR 2600
[redacted] **International Perspectives**	Meeting and Written Submission	Thursday, Oct. 18th @ 2:00pm	TBD

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Yahoo! Canada [redacted] **+ additional staff**	Meeting	TBD	
National Child Exploitation Coordination Centre (NCECC) **Earla-Kim McColl** **+ additional staff**	Meeting	TBD	
Canadian Association of Chiefs of Police (CACP) [redacted]	Written Submission; possible meeting (TBD)	TBD	

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.19(1)

DRAFT 04-Oct-07

[redacted]	Written Submission (via media comments); possible meeting (TBD)	TBD	
[redacted]	Written Submission via email		

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Still Awaiting Response: **B'nai Brith; Cybertip.ca** **Bell; Telus** **Canadian Association of Internet Providers (CAIP)** **Canadian Wireless Telecommunications Association (CWTA)** **IBM** **Canadian Bar Association** [redacted] **Canadian Information Processing Society**			

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Proposed List of Stakeholders for 2007 Consultation

It is recommended that the following individuals and groups be part of the proposed 2007 consultations on the customer name and address proposals.

Industry:

- Information Technology Association of Canada (ITAC)
- The Canadian Wireless Telecommunications Association (CWTA)
- Canadian Association of Internet Providers (CAIP)
- [redacted] Bell Canada
- [Industry Canada to propose additional participants]

s.19(1)

Consumer/Privacy Advocates/Academics:

- [redacted] – Ryerson University
- [redacted] – International Perspectives
- Raymond D'Aoust – Office of the Privacy Commissioner
- Canadian Bar Association
- [redacted] – Canadian Information Processing Society
- [redacted] – Professor (ENAP)
- [redacted] - Professor (University of Ottawa)

Law Enforcement/Victims and Crime Prevention:

- Royal Canadian Mounted Police (National Child Exploitation Co-ordination Centre)
- Canadian Association of Chiefs of Police (Law Amendments Committee)
- Ontario Provincial Police – Project "P"
- Cybertip.ca
- Canadian Resource Centre for Victims of Crime
- B'nai Brith

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Canadian Association of Chiefs of Police *Leading Progressive change in policing*
Association canadienne des chefs de police *À l'avant-garde du progrès policier*

June 1, 2009

The Right Honourable Stephen Harper, P.C., M.P.,
Prime Minister of Canada
Office of the Prime Minister
80 Wellington Street
Ottawa, ON K1A 0A2

Re: Modernization of Canada's Electronic Surveillance Laws (Lawful Access): Access to Subscriber Information

Prime Minister Harper,

I write urgently concerning the anticipated introduction of legislation concerning Canada's laws related to the lawful interception of private communications (Lawful Access). Over the past several years, the Canadian Association of Chiefs of Police (CACP) has consulted extensively with government and non-government stakeholders in an effort to move this much needed legislative reform forward.

As you know, Prime Minister Harper, the need to modernize our Lawful Access laws continues to be acute. Court ordered interceptions are a vital investigative tool used in the most serious and complex investigations. These include gang and organized crime investigations and other serious threats to public safety such as internet child exploitation.

One critical component of Lawful Access is the ability to access subscriber information, often referred to as Customer Name and Address information (CNA). This basic "non-core" biographical information held by telecommunication and internet service providers is a key building block in criminal investigations. There is now a substantial body of jurisprudence which supports the proposition that law enforcement access to this non-core biographical data does not require a warrant. In fact, most privacy statutes presently permit such disclosure to law enforcement agencies without a warrant.

582 Somerset Street West/582, rue Somerset Ouest, Ottawa, Ontario K1R 5K2
Tel: (613) 233-1106 • Fax/Télécopieur: (613) 233-6960 • E-mail/Courriel: cacp@cacp.ca

David H. Hill, C.M./Q.C., Lynda A. Bordeleau General Counsel/Conseillers juridiques
Perley-Robertson, Hill and McDougall LLP Barristers & Solicitors/Avocats et Procureurs

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

It is therefore critical that any legislation introduced by your government not place more onerous obligations on the police than are currently imposed by the courts. Any provision which would directly or indirectly impose a warranted regime for information is in our view, harmful to public safety. Such a requirement would impair effective and efficient criminal investigations and impose unnecessary and excessive costs on the police.

The CACP understands and is mindful of the privacy concerns of Canadians. We supported the Modernization of Investigative Techniques Act introduced in 2005, and the provisions in that Act allowing for access to CNA information without warrant. In our view those provisions reflected the existing state of the law and struck the appropriate balance between effective law enforcement and the privacy interests of Canadians.

We strongly urge your government to introduce effective Lawful Access legislation that balances the needs of effective law enforcement and national security investigations with the privacy rights of all Canadians. This requires that the legislation recognizes both the vital importance of CNA information and the present state of the law.

Sincerely,

[redacted] **s.19(1)**

cc: Honourable Peter Van Loan, Minister of Public Safety
Honourable Tony Clement, Minister of Industry
Honourable Robert Douglas Nicholson, Minister of Justice

582 Somerset Street West/582, rue Somerset Ouest, Ottawa, Ontario K1R 5K2
Tel: (613) 233-1106 • Fax/Télécopieur: (613) 233-6960 • E-mail/Courriel: cacp@cacp.ca

David H. Hill, C.M./Q.C., Lynda A. Bordeleau General Counsel/Conseillers juridiques
Perley-Robertson, Hill and McDougall LLP Barristers & Solicitors/Avocats et Procureurs

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

DRAFT 09-Oct-07

10034-7-3

CNA Consultations – Status and Planning Report

Groups	Method	Timing	Location
Federal Ombudsman for Victims of Crime **Steve Sullivan, Federal Ombudsman for Victims of Crime** **Louis Théorêt**	Meeting	Wednesday, Oct. 10th @ 1:00 – 2:15pm	269 Laurier 12th Floor, Section D BR D4700 (12ppl)
Canadian Resource Centre for Victims of Crime [redacted]	Meeting and possible written submission from NCECC	Wednesday, Oct. 10th @ 2:30 – 4:00pm	269 Laurier 17th Floor, Section B BR B2000 (16/34ppl)

s.19(1)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.19(1)

DRAFT 09-Oct-07

National Child Exploitation Coordination Centre (NCECC) **Earla-Kim McColl, Superintendent** **RCMP NCECC** **Susan Alter, RCMP Legal Counsel** [redacted]			
Ontario Provincial Police Child Pornography Section ("Project P") [redacted]	Conference Call	Thursday, Oct. 11th @ 1:00 – 2:30pm	269 Laurier 12th Floor, Section B BR B2600 (22ppl)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.19(1)

DRAFT 09-Oct-07

Rogers Communications [redacted] **+ 2 additional staff (wireless, security)**	Meeting	Friday, Oct. 12th @ 10:00 – 11:30am	269 Laurier 13th Floor, Section D BR D4400 (20ppl)
Information Technology Association of Canada (ITAC) [redacted] **+ additional members** **Canadian Wireless Telecommunications Association (CWTA)** [redacted]	Meeting; CWTA also to provide written submission	Friday Oct. 12th @ 2:30 – 4:00pm	269 Laurier 12th Floor, Section B BR B2600 (22ppl)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.19(1)

DRAFT 09-Oct-07

Office of Privacy Commissioner of Canada **Raymond D'Aoust, Assistant Privacy Commissioner** **+ 4 staff (policy, legal, etc.)**	Meeting	Monday, October 15th @ 2:00pm	269 Laurier 12th Floor, Section B BR B2600 (22 ppl)
[redacted] **International Perspectives**	Meeting and Written Submission	Thursday, Oct. 18th @ 2:00 – 3:30pm	269 Laurier 11th Floor, Section A BR A1600 (16ppl)
Yahoo! Canada [redacted] **+ additional staff**	Meeting	TBD	

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.19(1)

Canadian Association of Chiefs of Police (CACP) [redacted]	Written Submission; possible meeting (TBD)	TBD	
[redacted]	Written Submission (via media comments); possible meeting (TBD)	TBD	
[redacted]	Written Submission		

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Canadian Chamber of Commerce	Written Submission		
Canadian Internet Policy and Public Interest Clinic (CIPPIC) [redacted] **Additional written comments from** [redacted] **Law, Ethics and Technology at the University of Ottawa**	Written Submission		
<u>Still Awaiting Response:</u> **B'nai Brith; Cybertip.ca**			

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

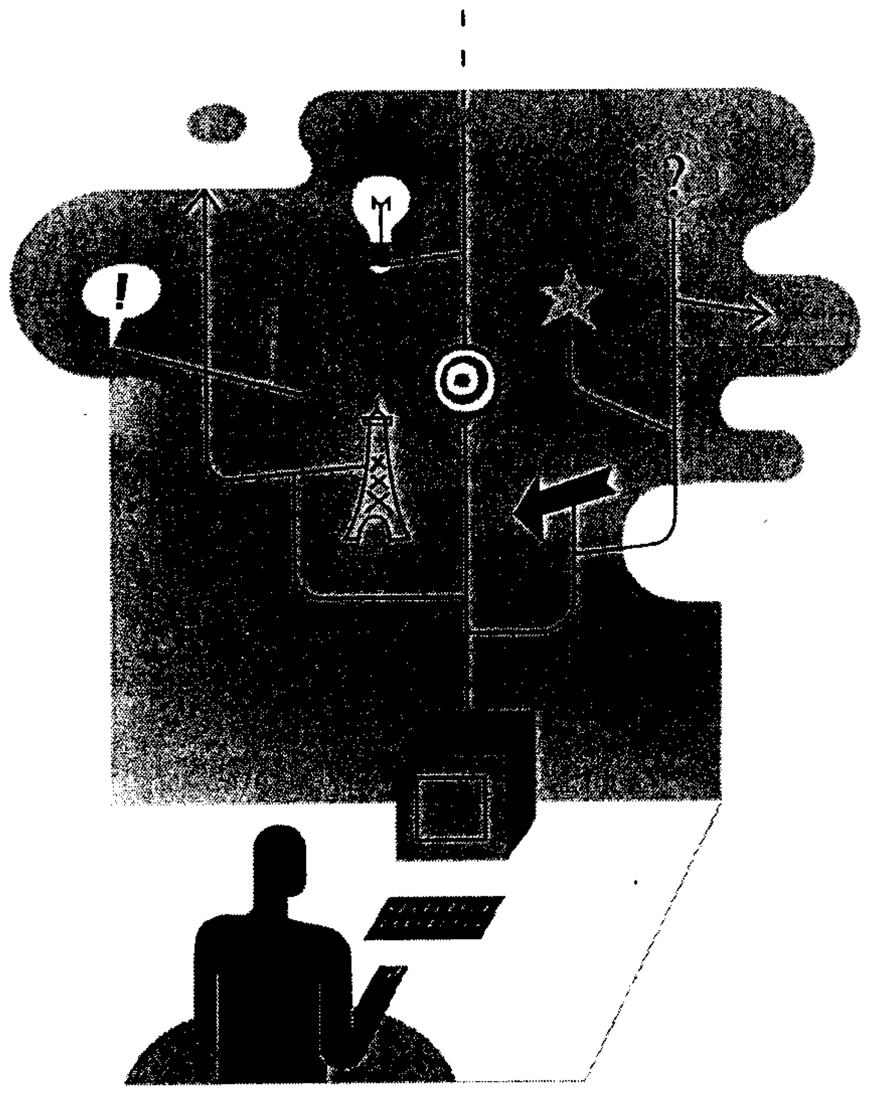
Bell; Telus; Videotron **Canadian Association of Internet Providers (CAIP)** **Canadian Advanced Technology Alliance (CATA)** **IBM** **Canadian Bar Association** **Electro-Federation of Canada** [redacted] **Canadian Information Processing Society**			

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

ITAC
INFORMATION TECHNOLOGY
ASSOCIATION OF CANADA

ACTI
ASSOCIATION CANADIENNE
DE LA TECHNOLOGIE DE L'INFORMATION

Customer Name and Address Consultation



October 2007

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

ITAC is the voice of the Canadian information and communications technologies industry in all sectors, including telecommunication and internet services, consulting services, hardware, microelectronics, software and electronic content. ITAC's network of companies accounts for more than 70 per cent of the 579,000 jobs, $137.6 billion in revenue, $5.2 billion in R&D investment, $22.6 billion in exports and $11.5 billion in capital expenditures that the industry contributes annually to the Canadian economy.

© 2007 Information Technology Association of Canada

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The Information Technology Association of Canada (ITAC) is pleased to respond to Public Safety Canada's discussion paper on customer name and address (CNA) information. The association has been actively involved in government consultations on lawful access to electronic communications since 2002.

Canada's telecom industry has a long history of working cooperatively with law enforcement within Canada's legal framework for lawful access, including access to customer information. All telecommunication service providers (TSPs) have developed some capability of responding to requests from law-enforcement agencies (LEAs) on a routine basis, and generally maintain dedicated security departments whose sole purpose is to respond to such requests and to comply with court orders. These services are provided at considerable cost to the TSPs.

Personal information associated with customers and subscribers of all telecom and internet services offered in Canada is subject to the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which allows TSPs to release a subscriber's personal information when compelled by law to do so. TSPs are also subject to CRTC rules regarding the protection of CNA information, although the specific rules vary among service types. In general, subscriber identifiers – aside from wireline telephone numbers – are expected to be treated as confidential and may be released only when TSPs are compelled by law to do so.

In order to comply with these rules regarding the protection of customer privacy, TSPs currently require a warrant or court order before providing LEAs with confidential customer information except in the most exigent circumstances. The discussion paper appears to suggest that Public Safety Canada is contemplating changes in the scope of CNA information and the circumstances and conditions under which TSPs would be compelled to collect certain specified CNA information and provide it LEAs. TSP obligations must be clearly set out in any new legislation or regulation, but as it is not clear to ITAC what exactly is under consideration we cannot respond in a more detailed fashion at this point.

As mentioned above, TSPs incur significant costs in responding to requests and providing lawful-access services to LEAs, and it is imperative that they be compensated for those costs. Industry concerns will only be exacerbated by a move to a "no warrant" regime – as raised in the discussion paper. The volume of requests for CNA information can be expected to increase substantially absent judicial oversight, with a corresponding substantial increase in costs to TSPs.

With respect to the specific kinds of CNA information, much of the wireline and wireless CNA information listed in the discussion paper is already available either publicly or via CRTC tariffed services. A variety of third parties provide "reverse look-up" services for Canadian telephone numbers and many of these are provided free of charge on the public internet. However, ITAC notes that the "basic identifiers" listed in the discussion paper go well beyond what most people would consider to be basic. IP addresses,

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

email addresses, IMSIs, ESNs, IMEIs and SIM numbers are not the "tombstone" data that is usually associated with CNA information. Nevertheless, ITAC is not aware of LEAs being unable to obtain the CNA information they require.

Any move to impose new requirements must take into account the fact that TSPs cannot always respond as quickly as may be desired. (For example, systems that provide quick response for directory assistance have not been developed for services other than wireline telephony.) Furthermore, while TSPs work diligently to respond to LEA requests, their ability to provide information is often constrained as a result of the volume of requests, the amount of detail required or other factors such as requests involving historical usage.

ITAC also notes that TSPs do not always have business reasons to collect CNA information, and so may not have in their possession the information sought by LEAs. ITAC would oppose the imposition of an obligation on TSPs to collect information that they would not be collecting for their own purposes. Significant service, business and cost issues would arise if carriers were required to collect, validate and maintain accurate CNA information simply for the purposes of lawful access.

In closing, ITAC acknowledges that lawful access and the ability to obtain CNA information are important tools for LEAs in their efforts to protect society. In its interventions on this issue, ITAC has consistently advocated for standards-based technical requirements, appropriate compensation for TSP costs and a phased-in approach to new obligations.

ITAC will not be able to support efforts to move ahead on this issue if our fundamental concerns continue to be left unaddressed – as they were in the previous legislative proposal, the *Modernization of Investigative Techniques Act*. To function properly, the Canadian lawful-access regime must recognise the realities of the telecommunication industry:

- TSPs must be compensated for the significant costs incurred responding to the requirements of LEAs.
- Any new technical requirements must be based on international standards, and provide an adequate phase-in period.
- The scope of CNA information and the circumstances under which it is to be provided by TSPs to LEAs must be explicitly identified and clarified in any new legislation or regulations.
- CNA information requirements must be applied in a technologically and competitively neutral fashion.
- TSPs must not be required to collect customer information beyond what is already collected for business purposes.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

ITAC appreciates the opportunity to share these comments and looks forward to the opportunity to comment on any specific legislative or regulatory amendments that are subsequently developed for consideration, especially if they go beyond the parameters of this consultation. We will of course also be pleased to meet with Public Safety Canada officials to discuss these issues.

As these matters are of considerable importance to Canadians, ITAC suggests that all written submissions to this public consultation be made available for public review on the Public Safety Canada website.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

10039-7-3

Federal Ombudsman for Victims of Crime Submission to the CNA Data Consultation Panel

October 10, 2007

Ottawa, Canada

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

FEDERAL OMBUDSMAN FOR VICTIMS OF CRIME
SUBMISSION TO CNA DATA CONSULTATION

The Office of the Federal Ombudsman for Victims of Crime was announced in March, 2006 by the Minister of Justice and the Minister of Public Safety. The mandate of the Federal Ombudsman for Victims of Crime relates exclusively to matters of federal responsibility and includes:

- facilitate access of victims to existing federal programs and services by providing them with information and referrals;
- address complaints of victims about compliance with the provisions of the *Corrections and Conditional Release Act (CCRA)* that apply to victims of offenders under federal supervision and provide an independent resource for those victims;
- enhance awareness among criminal justice personnel and policy makers of the needs and concerns of victims and the applicable laws that benefit victims of crime, including to promote the principles set out in the *Canadian Statement of Basic Principles of Justice for Victims of Crime*; and
- identify emerging issues and exploring systemic issues that impact negatively on victims of crime.

As part of our duty to alert the Government to emerging issues that impact negatively on victims of crime, we identified Internet facilitated child sexual exploitation as one of our main priorities. Despite the many positive aspects of the Internet for children, it has had a significant negative impact on some child victims of sexual abuse. We agree with the federal government that more needs to be done to identify and rescue children from ongoing sexual abuse and to prosecute those responsible for exploiting them.

The ability of police to identify and rescue children and to prosecute predators is essential. Many Internet Service Providers (ISPs) do cooperate with requests for information when police provide a letter of request. But according to the RCMP's

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

National Child Exploitation Coordination Centre, 30-40% of requests are denied. That means many predators go undetected, and many children are potentially left in abusive situations.

THE IMPACT OF INTERNET FACILITATED CHILD SEXUAL ABUSE

There are over 1 million child sexual abuse images on the Internet. Twenty thousand new pictures are added every week.[1] There are over 100,000 searches daily. There are tens of thousands of websites that promote sex with children.

The children seen in the images are getting younger and the abusers are getting more violent.[2] Over 85% of the children are under 12, many under 9 and almost one in five are under 3.[3] Eighty percent of the images involve penetration and 20% involve torture or bondage.[4]

Eighty percent of the abuse seen online is committed by people the children know.[5] Many of those who access and trade images are also abusers themselves. One study in the US found that 80% of offenders in prison for child pornography-related offences admitted to being abusers.[6]

---

[1] Unless otherwise stated, the statistics are provided by the RCMP's National Child Exploitation Coordination Centre.
[2] OPP Detective Inspector Angie Howe, *Senate Legal and Constitutional Affairs Committee*, Bill C-2, June 22, 2005.
[3] http://www.mg.co.za/articlePage.aspx?articleid=320210&area=/insight/insight__international/
[4] CTV.ca, July 23, 2006.
[5] C-CAICE
[6] Dr. Peter Collins, *Standing Committee on Justice and Human*, Bill C-2, May 3, 2005.

000097

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Therapists, law enforcement and victim services have years of experience dealing with child sexual abuse victims, but there is growing recognition that child sexual abuse images and the Internet complicate the impact of the offences, the recovery of victims and the delivery of services. Tink Palmer, a member of *Stop it Now! UK*, asserts that, "…we need a radical reconsideration of current practices, policies and procedures in the light of new technological conduits for abusing children."[7]

She goes on to say, "the additional trauma for a child who knows that their humiliation has been photographed or filmed, and that people around the world may access and witness it in the immediate present and also long into the future, has serious and complex implications for assisting the child's recovery and for the way such crimes are investigated."[8]

End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes' (ECPAT) contends, "Child pornography amplifies and broadcasts the original act of abuse that it depicts. In doing so, it can substantially aggravate the original offence."[9]

One child sexual abuse victims whose photos were put on the Internet said, "Usually, when a kid is hurt and the abuser goes to prison, the abuse is over. But because XXX put

---

[7] Tink Palmer, "Abusive images: The impact on the child," in ECPAT Newsletter, Issue 49 1/January/2005.
[8] Tink Palmer, "Abusive images: The impact on the child," in ECPAT Newsletter, Issue 49 1/January/2005.
[9] John Carr, "Theme Paper on Child Pornography for the 2nd World Congress on Commercial Sexual Exploitation of Children" p.13
http://www.ecpat.net/eng/Ecpat_inter/projects/monitoring/wc2/yokohama_theme_child_pornography.pdf

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

my pictures on the Internet, the abuse is still going on…I am more upset about the pictures on the Internet than I am about what XXX did to me physically."[10]

Another victim said, "I never escape the fact that pictures of my abuse are out there forever. Everything possible should be done to stop people looking at pictures of child abuse. Each time someone looks at pictures of me, it's like abusing me again."[11]

The Supreme Court of Canada, in the case of *R. v. John Robin Sharpe*, said,

> "The child is traumatized by being used as a sexual object in the course of making the pornography. The child may be sexually abused and degraded. The trauma and violation of dignity may stay with the child as long as he or she lives…the child must live in the years that follow with the knowledge that the degrading photo or film may still exist, and may at any moment be being watched and enjoyed by someone."[12]

Victims often do not disclose that photos were taken or videos were made, and even when confronted with such discoveries, some victims will refuse to acknowledge that this was done. "Practitioners report that a child in this situation may feel that the existence of imagery of their humiliation masks the violence they have experienced and makes them appear complicit. This dilemma adds an extra traumatic burden…Anxiety may intensify where a child understands that images of their abuse will continue to be replicated and circulated to an audience that is both nearby and global long into the future."[13]

---

[10] Julian Sher, *One Child at a Time*, 2007
[11] Julian Sher, *One Child at a Time*, 2007
[12] R. v. Sharpe, [2001] 1 S.C.R. 45, 2001 SCC 2, paragraph 92.
[13] ECPAT International, "Violence Against Children in Cyberspace," 2005. p.41

000099

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Children may have difficulties accepting that they cannot control their images; that once they are on the Internet, men around the world may be using them for their own sexual gratification or to groom other children. They must learn to live with the reality that their photos will be on the net and in people's computers forever. ECPAT says,

> "...even where it has been possible to identify a victim, the chances of being able to help the child to recover from the trauma of the initial involvement in the abuse can be seriously compromised if the child learns or comes to believe that images of them engaged in the abusive behaviour might have been scanned, or converted into a digital format in some other way, for storage on a computer or for transmission between computers e.g. over the Internet. This, in effect, makes the image part of a permanent public record. It could, even randomly, suddenly appear on the screen of their next-door neighbour or classmates."[14]

FEDERAL GOVERNMENT'S COMMITMENT TO CHILDREN

There can be little doubt that this Government has repeatedly displayed its commitment to protect children from those who would prey on them. Bill C-22, which would raise the age of consent from 14 to 16, is but one example.

That commitment was also evident in the 2007 Budget, when the Minister of Finance gave an additional $6 million to the RCMP to protect children from sexual exploitation. Minister Flaherty said, "The funding will ensure that those who commit these heinous offences are brought to justice..."

In 2003, the Government of Canada signed the *Canadian Basic Statement of Principles for Victims of Crime*, which commits the federal government to consider and respect the

---

[14] John Carr, "Theme Paper on Child Pornography for the 2nd World Congress on Commercial Sexual Exploitation of Children" p.14
http://www.ecpat.net/eng/Ecpat_inter/projects/monitoring/wc2/yokohama_theme_child_pornography.pdf

000100

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

privacy of victims to the greatest extent possible; to minimize inconvenience to victims and to take appropriate measures to protect victims. Canada is also a signatory to several key UN declarations that speak to the need to protect and promote the safety and privacy of victims and children.

More recently, Canada with other G8 Ministers agreed to accelerate efforts to combat child sexual exploitation. The G-8 Ministers committed, "to ensuring the implementation and effectiveness of our own laws relating to child pornography, and to taking steps to update and improve those laws when necessary and where appropriate."[15] The Ministers also acknowledged and recognized that the private sector, including Internet Service Providers (ISPs), have a role to play in protecting the world's children." The Ministers recognized that, "Child pornography grievously harms all children: it harms the child who is sexually assaulted in the making of the image; the same child is re-victimized every time that image is viewed."[16]

THE LAWFUL ACCESS DEBATE

For years, the law enforcement community has been calling upon the federal government to reform the *Criminal Code* to enable them to apply real world police tools to the virtual world. For example, police can get a customer's name from a telephone company, but not from an Internet Service Provider (ISP). After a series of consultations, the former government introduced Bill C-74, which among other things (that will not be discussed

---

[15] G-8 Justice and Home Affairs Ministers, May 24, 2007. www.g8.gc.ca/childpornography-en.asp
[16] G-8 Justice and Home Affairs Ministers, May 24, 2007. www.g8.gc.ca/childpornography-en.asp

000101

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

here in any detail) enhanced law enforcement's capability to access customer name and address (CNA) information from ISPs. Although the bill had problems,[17] it was seen as a welcome initiative by those concerned with law enforcement and the protection of children from Internet sexual predators. Bill C-74 died on the Order Paper when the election was called.

Subsection 7(3)(c) of the *Personal Information Protection and Electronic Documents Act (PIPEDA)* sets out provisions where an organization **may** disclose personal information without consent. It refers 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.

Parliament clearly intended to facilitate the enforcement of criminal law, but the Committee heard that law enforcement has found it to be a hindrance. Of particular concern is with respect to investigations of suspected Internet facilitated child sexual exploitation. Some ISPs do cooperate with law enforcement requests in child sexual abuse investigations, in part because they recognize the uniqueness of the child pornography[18] provisions in the *Criminal Code* - that it is a crime to simply access and view child sexual abuse images. That makes it somewhat different than other crimes. For

---

[17] For example, the bill allowed companies exceptions if it was cost prohibitive. This is not consistent with other industries. Government does not allow the car industry to only take safety measures if they can afford it. When municipalities impose smoking bans on restaurants and establishments, there are no exceptions for establishments that might suffer a financial hardship.

[18] Generally, we prefer to use the term child sexual abuse images (CSAI) rather than child pornography because CSAI is more reflective of what it is we are talking about – permanent records of child abuse. We a woman is raped, we do not call it adult pornography. We should not do it when it comes to children.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

example, it is not illegal simply to read hate literature. Unfortunately, not all ISPs cooperate with law enforcement.

The Standing Committee on the Access to Information, Privacy and Ethics conducted a widespread review of the *Personal Information Protection and Electronic Documents Act (PIPEDA)* during the last year. It released its Fourth Report earlier this year.

Mr. Clayton Pecknold of the Canadian Association of Chiefs of Police testified before the Committee and explained the challenges the police currently face:

> "...we are increasingly seeing some companies interpreting lawful authority to mean that a warrant or court order is required before they comply. This is an interpretation that is not, in our respectful view, consistent with the intent of the drafting of the act. Such an interpretation by companies, while no doubt grounded in a legitimate desire to protect their customers' privacy, is overly restrictive and defeats, in our view, the intent of paragraph 7(3)(c.1). (February 13, 2007)

On August 16, 2007, I wrote to the Honourable Jim Prentice, Minister of Industry, in relation to *Recommendation #12* of the Committee's Report, which is relevant to this consultation as it reflects the will of the committee and was a unanimous recommendation, indicating support for the recommendation from all parties. The recommendation states,

> "*The Committee recommends that consideration be given to clarifying what is meant by "lawful authority" in section 7(3)(c.1) of PIPEDA and that the opening paragraph of section 7(3) be amended to read as follows: "For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization shall disclose personal information without the knowledge or consent of the individual but only if the disclosure is [...]*"

000103

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The Committee agreed that it is not realistic or necessary to expect police to seek a warrant in these situations. By including subsection 7(3)(c.1), Parliament clearly did not intend for law enforcement to secure a warrant for information that is not considered personal.

IS CNA PERSONAL INFORMATION?

Recently, the Federal Court ruled that EBay had to give personal information about high volume sellers' clients to the Canada Revenue Agency in order to ensure that those individuals are paying the appropriate taxes.[19]

Courts have said that people do not have a reasonable expectation of privacy attributed to their name and address. In *R v. Plant,*[20] the Supreme Court said,

> "The police check of computerized records was not unreasonable...In view of the nature of the information, the relationship between the accused and the electrical utility, the place and manner of the search and the seriousness of the offence under investigation, it cannot be concluded that the accused held a reasonable expectation of privacy in relation to the computerized electricity records which outweighed the state interest in enforcing the laws relating to narcotics offences. While they reveal the pattern of electricity consumption in the residence, the records do not reveal intimate details of the accused's life. Since the search does not fall within the parameters of s. 8 of the *Charter*, this information was available to the police to support the application for a search warrant."[21]

The Court of Queen's Bench of Alberta said, "there is no reasonable expectation of privacy with respect to: 1. General banking information - see *R.* v. *Lillico* (1994), 92

---

[19] Paul Waldie, Taxman goes browsing on eBay, Globe and Mail, September 27, 2007
[20] *R. v. Plant*, [1993] 3 S.C.R. 281. This case dealt with marijuana grow-ops and the police obtained information from the electricity company regarding the owner's electricity use.
[21] R. *v.* Plant, [1993] 3 S.C.R. 281

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

C.C.C. (3d) 90 (Ont. Gen Div.); [1999] O.J. No. 95 (Ont. C.A.); 2. Cellular telephone records - see *R.* v. *Brown,* [2000] O.J. No. 1177 (Sup. Ct. Jus.) at para.63."[22]

In *R. v. Quinn,* in which police requested "tombstone" information regarding several accounts in which cheques had been deposited, the BC Court of Appeal said, "there was no search, much less any unreasonable search as envisioned in the *Charter.*"[23]

If EBay has to give the Canada Revenue Agency the names and addresses of citizens to make sure that taxes are paid, does it not seem strange that Internet Service Providers (ISP) do not have to give the same information to the police trying to find a sexual predator who may be abusing a child? Measures to prevent a predator from abusing a child should be given the same priority as collecting unpaid taxes.

This is not a privacy issue. It is a public safety issue. It is a child safety issue.

Some have suggested that police should be required to get a warrant for this information. This is inconsistent with the view of the courts which have said this kind of information is not personal. This is, after all, information that can be found with a license plate, phone book or driver's license. The reality of Internet facilitated child exploitation investigations is that children may be at immediate risk. Most abusers seen in online abuse images know the child; many are related; and therefore they have ongoing access to the child.

---

[22] *R. v. Haskell*, 2004 ABQB 474
[23] *R. v. Quinn* 2006 BCCA 255 paragraph 93

000105

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

In 2004, Michael Briere murdered 10 year old Holly Jones minutes after looking at child sexual abuse images online. He walked out of his home and saw the young girl walking down the street. He grabbed her, took her into his home where he sexually assaulted her before killing her and taking steps to dispose of her remains. At his sentencing hearing, Briere told the court he was consumed by desire after viewing child pornography.[24] While this is an extreme example of what can happen, it should be an important reminder to all of us. Law enforcement officers are increasingly seeing children being abused live on the Internet. And none of us know what happens when the predator turns the computer off. He might not do what Michael Briere did, but it is not a leap of logic to suggest a child might be at risk of further abuse.

It is not acceptable to demand law enforcement to waste their valuable time and resources, not to mention the court's time and resources, to get a warrant for information that the Canada Revenue Agency can demand from EBay. This is information they can demand of someone they see jaywalking or through the license plate of someone seen driving away from a car accident. Preventing child sexual abuse and tracking abusers is as important as preventing traffic accidents and enforcing street laws.

The suggestion that law enforcement secure a warrant for CNA assumes law enforcement can get a warrant in these circumstances, which may not be the case. It is not a question of inconvenience or making a police officer's job easier; it is about rescuing children.

---

[24] CBC News Online, http://www.cbc.ca/news/background/jones_holly/

000106

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The government's Consultation Paper says, "If the custodian of the information is not cooperative when a request for such information is made, law enforcement agencies *may have no means to compel the production of information pertaining to the customer…The availability of such building-block information is often the difference between the start and finish of an investigation.*"

The good news is that many ISPs are cooperating with police without a warrant, although it remains to be seen what the impact of the Minister's recent comments will be on those companies.

The bad news is requests are denied 30 to 40% of the time.[25] That means 30% of investigations might end on the starting block, and children at risk are left in those abusive situations. Even if the number was lower, it still would not be acceptable. It is unacceptable that we leave a child in an abusive situation one day longer than necessary. Those children must not be sacrificed for the misplaced concern for individual privacy.

The recent debate has created the perception that police want more than just CNA; that they want access to emails. It has also left people with the mistaken belief that police can easily get a warrant in these circumstances. The reality is quite different.

This is what law enforcement refer to as the pre-warrant stage. It is the beginning of an investigation and they need a name to begin the investigation. If they get a name and find out, for example, that John Doe has a 5 year old girl who matches the description of the

[25] RCMP's National Child Exploitation Coordination Centre

000107

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

images they found online, then they might knock on John's door and save that little girl from being raped that night. But if they cannot get John Doe's name and address, they will not rescue that child.

It is important to note that getting CNA does not mean that the customer is the perpetrator. It does not place him/her in front of the computer at the time the images were traded (for example). An investigation will be required to determine that. But again, it begins with a name and address.

Other countries, including the UK, Australia and the US, do not require law enforcement to secure a warrant before accessing CNA from an ISP. In fact, the scheme set out in Bill C-74 appeared to be more restrictive than that of the other three countries."[26]

WHAT ABOUT THE PRIVACY OF THE CHILD?

At the risk of being repetitive, this is not a privacy issue but a child safety issue. It is unfortunate, given that the debate has focused so much on privacy, that not one word has been spoken about the privacy interests of the children whose images are being traded like baseball cards. The *Canadian Statement of Basic Principles of Justice for Victims of Crime* requires the federal government to consider the privacy interests of victims.

---

[26] Dominique Valiquet, Telecommunications and Lawful Access: II. The Legislative Situation in the United States, the United Kingdom and Australia, 28 February 2006, Library of Parliament, http://www.parl.gc.ca/information/library/PRBpubs/prb0566-e.html.

000108

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The Supreme Court said,

> "Child pornography also undermines children's right to life, liberty and security of the person as guaranteed by s.7....We recognize that privacy is an important value underlying the right to be free from unreasonable search and seizure and the right to liberty. However, the privacy of those who possess child pornography is not the only interest at stake in this appeal. The privacy interests of those children...are engaged by the fact that a permanent record of their sexual exploitation is produced."[27]

Is there any more serious privacy violation than to allow images of a child being raped to be distributed to hundreds of thousands of sexual predators? Imagine growing up knowing those photos are available forever, for anyone to see, and you have no control over them. It should put the controversy over releasing a name in perspective.

CONCLUSION

This debate is not about increasing police powers or the Government's ability to monitor people's activity on the web. It is about rescuing children from potentially abusive situations and prosecuting those who might be abusing and exploiting them.

Everyday, police officers across the country sit in front of computers and sift through tens of thousands of images and watch videos of the most horrific abuse imaginable. They hear the screams of pain. They see the tears.

---

[27] R. v. Sharpe, [2001] 1 S.C.R. 45, 2001 SCC 2, paragraph 189.

000109

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

If society is going to ask them to do this work, they need to give them the tools to finish the job. Not for the police, not to make their job easier, but for the children.

During a presentation at the NCECC/OPP recent conference, a short audio clip of a little girl being raped by her father.[28] She said, "Daddy, it hurts. It hurts so bad."

What if police needed CNA to help find her but the ISP said no and they could not get a warrant? It is unspeakable that a father would do that to his child, but it would be unforgivable if he was allowed to do it again.

[28] The presenter was illustrating how new software can be used to enhance sound.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

RECOMMENDATIONS:

As Federal Ombudsman for Victims of Crime, I recommend the federal government enact legislation requiring ISPs to provide CNA information to law enforcement investigating Internet facilitated child sexual abuse cases. Legislation is necessary to clarify that a judicial authorization is not necessary and that the current practice in which many ISPs accept written requests for CNA from authorized law enforcement officers investigating Internet facilitated child sexual abuse be adopted.

Furthermore, in addition to audit results being provided to the Privacy Commissioner (as was proposed in the consultation document), I recommend that audit results also be provided to the Federal Ombudsman for Victims of Crime.

000111

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.
IOS 34-7-3

Response of the Office of the Privacy Commissioner of Canada to the Customer Name and Address (CNA) Information Consultation Document

October 2007

The Rationale for the Consultation

According to the consultation document issued by Public Safety Canada and Industry Canada, "The objectives of this process are to maintain lawful access for law enforcement and national security agencies in the face of new technologies while preserving and protecting the privacy and other rights and freedoms of all people in Canada."[1]

The consultation document is based on the assumption that law enforcement and national security (LE/NS) agencies are experiencing difficulties obtaining access to customer name and address (CNA) information in a timely way. The consultation document sets out the problem as follows:

> Law enforcement agencies have been experiencing difficulties in consistently obtaining basic CNA information from telecommunications service providers (TSPs). In the absence of explicit legislation, a variety of practices exists among TSPs with respect to the release of basic customer information, e.g., name, address, telephone number, or their Internet equivalents. Some companies provide this information voluntarily, while others require a warrant before providing any information, regardless of its nature or the nature of the situation. If the custodian of the information is not cooperative when a request for such information is made, law enforcement agencies may have no means to compel the production of information pertaining to the customer. This poses a problem in some contexts. For example, law enforcement agencies may require the information for non-investigatory purposes (e.g., to locate next-of-kin in emergency situations) or because they are at the early stages of an investigation. The availability of such building-block information is often the difference between the start and finish of an investigation.

The excerpt above suggests that the problem is one of inconsistency; some TSPs provide this information voluntarily while others are unwilling to provide this information or will do so only in response to a warrant.

The consultation document states "This poses a problem in some contexts" and it goes on to refer to two situations where problems arise. The first involves the use of CNA information for non-investigative emergency purposes; the second involves the use of CNA information during the early stages of an investigation.

---

[1] The consultation document is available at http://securitepublique.gc.ca/prg/ns/cna-en.asp

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Unfortunately the consultation document does not provide any sense of the scope of the difficulties mentioned in the document. Are 80 per cent of TSPs providing CNA information voluntarily or is the figure 20 per cent? Are telephone companies more likely to provide the information than Internet service providers (ISPs)? Are small TSPs more likely to request a warrant? Nor does the consultation document indicate whether TSPs respond differently depending on the situation. For example, do TSPs respond differently to next-of-kin emergency situations than they do to requests involving suspected violent crimes?

Requiring all TSPs to disclose CNA information on request is an overly broad, one size fits all response to a problem that has not been clearly defined or measured. We raised this issue in response to the 2002 consultation and the 2005 consultation on lawful access:

> When the 2002 Consultation Paper on Lawful Access was issued by the Department of Justice, Industry Canada and the Solicitor General, our Office, along with several other parties, questioned the need to revise the existing lawful access regime. We pointed out that the departments had failed to demonstrate the existence of a serious problem that needed to be addressed. We urged the three departments to present a clear statement of the problems that law enforcement agencies were encountering along with empirical evidence supporting the need for enhanced surveillance powers proposed in the consultation paper.
>
> This has still not been done. Without a clear understanding of the problems that the proposed legislation is intended to correct it is impossible for our Office or the Canadian public to determine if the measures being proposed are necessary and proportionate.

Although the current consultation addresses only some of the issues raised in previous consultations, the comments we made in 2005 are still appropriate.

The *Personal Information Protection and Electronic Documents Act (PIPEDA)*

As federal works, undertakings and businesses (FWUBs) all TSPs operating in Canada are subject to *PIPEDA* even if they only provide service in a province with substantially similar legislation.

PIPEDA requires that organizations obtain consent for disclosures of personal information subject to a limited number of exceptions. Three of the exceptions are particularly relevant to the issues raised in the consultation document:

- Under paragraph 7(3)(c) an organization may disclose information without consent when it is required to comply with a subpoena, a warrant or a court order;
- Under paragraph 7(3)(c.1), an organization may disclose personal information to a government institution, including a law enforcement agency,

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

for the purpose of enforcing a law, carrying out an investigation, gathering intelligence for the purpose of enforcing a law, or administering a law; and

- Paragraph 7(3)(e) allows disclosures without consent to a person who needs the information because of an emergency that threatens the life, health or security of the an individual.

Paragraph 7(3)(c) deals with mandatory disclosures pursuant to a legal authorization.

Paragraph 7(3)(c.1), in contrast, is clearly intended to allow organizations to disclose personal information without consent or notification to LE/NS agencies and other government bodies in the absence of prior judicial authorization. However, the organization requesting the information has to identify its legal authority and indicate that it is collecting the information for one of the reasons listed in the paragraph, for example to enforce a law of Canada, a province or a foreign jurisdiction.

When the legislation (Bill C-6) was being debated in the House of Commons, the Minister of Industry clearly stated that 7(3)(c.1) was intended to maintain the *status quo*. "These amendments do not grant new powers to government institutions, nor do they create new obligations on business." Although 7(3)(c.1) was not intended to alter the *status quo* we appreciate that it may have created some uncertainty on the part of organizations being asked to disclose certain information.

This provision was the subject of a considerable amount of discussion during the mandatory five year review of *PIPEDA* conducted by the House of Commons Standing Committee on Access to Information Privacy and Ethics. In its report, tabled on May 2, 2007, the Committee recommended that consideration be given to clarifying what is meant by 'lawful authority' in section 7(3)(c.1). The Committee also recommended changing the "may" in the opening paragraph of subsection 7(3) to "shall" which seemingly would have made all the disclosures in 7(3) mandatory.

In its response to the Committee's report, table on October 17, 2007, the government indicated that there is a need to clarify the concept of lawful authority. The government rejected the Committee' recommendation about changing "may" to "shall."

The government's response also sought to clarify the overall intent of the paragraph:

> The government wishes to confirm that the purpose of s. 7(3)(c.1) is to allow organizations to collaborate with law enforcement and national security agencies without a subpoena, warrant or court order. Organizations who share information with government institutions, including law enforcement and national security agencies, in accordance with the requirements of this provision, are doing so in compliance with *PIPEDA*.

The government also indicated that it will examine the possibility of adding a regulation to further define the term "government institution" that is found in 7(3)(c.1) and 7 (3)(d).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Although neither the Committee's report nor the government's response directly referred to 7(3)(e), the government's response stated that it would consider certain limited exceptions to *PIPEDA*'s consent requirements to address the concerns expressed by stakeholders regarding the disclosure of personal information in cases of natural disasters, elder abuse and other similar circumstances. Such a change would undoubtedly be relevant to the issue of disclosing CNA information to LE/NS agencies for emergency purposes.

As the consultation document suggests, at least some of the difficulties that LE/NS agencies face in terms of obtaining CNA information is one of inconsistency. The changes that the government is proposing to make to *PIPEDA* as a result of the five year review may go a long way towards clarifying when and how TSPs may disclose CNA information under 7(3)(c.1) and possibly 7(3)(e).

The Privacy Commissioner has stated publicly that she would not object to adding definition for the terms "lawful authority" and "government institution" if the government feels that such definitions would bring clarity to the legislation.

Although the consultation paper identifies the "absence of explicit legislation" as one of the problems the consultation process seeks to address, *PIPEDA* is, in fact, an explicit legislative code that permits lawful access by LE/NS agencies while "preserving and protecting the privacy and other rights and freedoms of all people in Canada." Before considering legislation that would make the disclosure of CNA mandatory on request, we would strongly recommend that the government determine if the clarification to *PIPEDA* discussed above, together with any guidance that may be appropriate, address the inconsistency. In terms of guidance, Service Alberta has produced a guidance document, "Requesting Personal Information from the Private Sector: Forms and Guidelines for Law Enforcement Agencies", that includes two forms that law enforcement agencies can use when requesting personal information from organizations.[2]

CNA and the Expectation of Privacy

The Consultation document does not define CNA information, but it states that it could include "the following basic identifiers associated with a particular subscriber":

- name;
- address(es);
- ten-digit telephone numbers (wireline and wireless);
- Cell phone identifiers, e.g., one or more of several unique identifiers associated with a subscriber to a particular telecommunications service (mobile identification number or MIN; electronic serial number or ESN; international mobile equipment or IMEI number; international mobile subscriber identity or IMSI number; subscriber identity module card number of SIM Card Number);
- e-mail address(es);

[2] See http://www.pipa.gov.ab.ca/resources/pdf/forms_and_guidelines_for_law_agencies.pdf

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- IP address; and/or,
- Local Service Provider Identifier (LSPID), i.e., identification of the TSP that owns the telephone number or IP address used by a specific customer.

Referring to all of this information as customer name and address information is misleading, as is calling these data elements "basic identifiers." This list goes well beyond the customer names and addresses associated with a given telephone number. Some of this information is available through white page directories and reverse directories. However, much of this information is not publicly available; furthermore, much of this information would be unknown to the individuals involved. For example, many people with Internet service do not know their IP address. Similarly, many cell phone subscribers would not even know that there are any identifiers associated with their telephone other than the number.

The assumption behind the consultation paper is that CNA information carries a low expectation of privacy and as such does not require judicial authorization. We disagree: many individuals consider much of this information to be private. First of all, a significant number of people choose to pay extra for unlisted telephone numbers, demonstrating that they consider these numbers to be private. Many people only share their cell phone numbers with friends and family numbers. One of the attractions of the Internet is that it provides an expectation of privacy. Many people use pseudonyms on the Internet in order to engage in anonymous communications and for a variety of other reasons.[3]

In *BMG et al v. John Doe et al* Justice von Finckenstein concluded that it would irresponsible for the Court to order disclosure of the name of an account holder given the uncertainty that exists about the link between the identity of an account holder and an anonymous user as well as the link between the user of an account and a given dynamic IP address.[4]

While some of the this information might be considered less sensitive we need to recognize that it is typically not being sought as an end in itself. CNA information may be valuable to LE/NS agencies specifically because it can provide access to even more sensitive information.

---

[3] See Wilkins J. in *Irwin Toy Ltd. v. Doe* (2000), 12 C.P.C. (5th) 103 (Ont. Sup. Ct.) at paragraphs 10-11: "Implicit in the passage of information through the internet by utilization of an alias or pseudonym is the mutual understanding that, to some degree, the identity of the source will be concealed. Some internet service providers inform the users of their services that they will safeguard their privacy and/or conceal their identity and, apparently, they even go so far as to have their privacy policies reviewed and audited for compliance. Generally speaking, it is understood that a person's internet protocol address will not be disclosed. Apparently, some internet service providers require their customers to agree that they will not transmit messages that are defamatory or libellous in exchange for the internet service to take reasonable measures to protect the privacy of the originator of the information."

[4] *BMG Canada Inc. v. John Doe* [2004] 3 F.C.R. 241.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Section 8 of the Charter of Rights and Freedoms protects Canadian against unreasonable search and seizure when there is a reasonable expectation of privacy. The Supreme Court has recognized that an individual's expectation of privacy may depend on location, the nature of the information and the relationship of the information to the individual. On the third point, one criterion the Court uses in deciding if an individual has a reasonable expectation of privacy is whether the personal information involves "a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state".[5]

In *R v. Plant*, where this concept of "a biographical core of personal information " was first used, the Court found that electricity consumption records did not meet this biographical core test. One consideration used by the Court in reaching this conclusion was that this information is generally accessible by the public. This is not the case with unlisted numbers and cell phone numbers which are fiercely protected by many people indicating a strong expectation of privacy.

In a strong dissenting judgment in *R. v. Plant*, Justice McLachlin (as she then was) noted that

> [c]omputers may and should be private places, where the information they contain is subject to legal protection arising from a reasonable expectation of privacy. Computers may contain a wealth of personal information. Depending on its character, that information may be as private as any found in a dwelling house or hotel room.[6]

Many, if not all, of the various types of personal information included within the ill-named category of "customer name and address" information constitute personal information to which a reasonable expectation of privacy attaches. We strongly recommend that due consideration be given to the *Charter* implications of any legislation that would make it mandatory for a TSP to disclose this personal information when confronted with a warrantless request that is, in reality, a demand.

Proposed Safeguards

The paper proposes a number of safeguards that could be implemented if the government decided to require TSPs to disclose CNA information on request. However, these safeguards only become relevant if one accepts that mandatory disclosure is an appropriate and necessary solution.

We do not propose to comment on the proposed safeguards in any detail. We will comment more fully on possible "checks and balances: and oversight models if legislation is introduced implementing these proposals.

---

[5] *R. v. Plant*, [1993] 3 S.C.R. 281.
[6] *Ibid.*, para. 45.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The consultation paper suggests that agency heads be required to conduct regular internal audits to ensure that any requests for CNA information are being made in accordance with the protocols and safeguards in place. The paper goes on to suggest that audit results be submitted to the Privacy Commissioner of Canada, the Security Intelligence Review Committee, or provincial privacy commissioners, as appropriate.

The paper also refers to explicit provisions to allow the Privacy Commissioner and the Security Intelligence Review Committee to conduct audits related to the release of CNA information.

While after the fact audits are an important means of assessing compliance, they are not a substitute for prior authorization. With respect to our ability to conduct audits with respect to the disclosure of CNA information, our Office can conduct a compliance review of a government department or agency at any time at the discretion of the Commissioner under section 37 of the *Privacy Act*,. Under section 18 of *PIPEDA* we require "reasonable grounds to believe" that an organization is contravening the Act before we can conduct an audit. Although some provincial commissioners may have the authority to audit a provincial or municipal police force in terms of compliance with provincial privacy legislation they do not all have this authority, or the resources to conduct such a review. It is not apparent how the federal government could require a provincial or municipal police force to maintain audit records. This would potentially leave a significant gap in terms of oversight.

Conclusion

The consultation paper is based on a number of assumptions:

1. LE/NS agencies are experiencing difficulties in obtaining access to CNA information that are sufficiently serious to justify new privacy intrusive measures;
2. there is no reasonable expectation of privacy in CNA data; — NO. just that it can be met w/ safeguards
3. requiring TSPs to disclose this information on request is necessary to address these difficulties; and
4. this approach preserves and protects "the privacy and other rights and freedoms of all people in Canada", as the consultation paper suggests.

We are not convinced that these assumptions are sound. First of all, we do not have a clear sense of the seriousness of the problem. Neither this consultation paper nor previous consultation documents has presented a compelling case based, on empirical evidence, that the inability to obtain CNA in a timely way has created serious problems for LE/NS agencies in Canada. This calls into question the policy rationale from both a proportionality and necessity perspective. Second, it is our view that a reasonable expectation of privacy attaches to CNA data. This renders any mandatory disclosure/seizure regime of dubious constitutional validity. // euro also - but this does not mean we need a warrant

Assuming there is a well documented and empirically demonstrated problem in obtaining access to CNA information, we are not convinced that requiring TSPs to

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

well what else can we expect given we've said repeatedly we want an investigation

disclose this information without a warrant is the only solution or the most appropriate solution. As discussed above, clarifying *PIPEDA* and providing guidance, may go a long way towards resolving this matter. We would also point out that the Canadian Radio-television and Telecommunications Commission (CRTC) has already addressed the issue of access to provider information (LSPID) by law enforcement agencies in Telecom Decision CRTC 2002-21[7]. In that decision the CRTC determined in order to obtain LSPID, a law enforcement agency had to identify its lawful authority to obtain the information and indicate that

1. it has reasonable grounds to suspect that the information relates to national security, the defence of Canada or the conduct of international affairs;
2. the disclosure is requested for the purpose of administering or 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 or administering any such law; or
3. it needs the information because of an emergency that threatens the life, health or security of an individual, or the law enforcement agency otherwise needs the information to fulfill its obligations to ensure the safety and security of individuals and property.

The CRTC's decision uses language similar to that found in subsection 7(3) of *PIPEDA* with the significant addition of the reference to "reasonable grounds to suspect". The CRTC's approach should also be considered.

Finally, we agree with the consultation paper that "the principles and powers of lawful access must be exercised in a manner consistent with the rights and freedoms guaranteed in the *Canadian Charter of Rights and Freedoms*." However, we are not convinced that allowing LE/NS agencies to obtain CNA information on demand would meet this threshold. As discussed above, we do not accept the premise that individuals have a low expectation of privacy with respect to the information in question and that obtaining this information without judicial authorization would protect "the privacy and other rights and freedoms of all people in Canada."

? why are they giving Charter advice? I'm well.

too bad.

---

[7] Telecom Decision CRTC 2002-21, 12 April 2002, Provision of subscribers' telecommunications service provider identification to law enforcement agencies.