Simplifying Lawful Access – Bill – C-30 – Through the Lens of Law Enforcement

Introduction:

When law enforcement uses words such as electronic interception, intercept capable, electronic surveillance and combines such words with the most widely used forms of communications by society – Internet, cellulars, social media.....it understandably raises concerns of many Canadians. So much so that when Canada's Privacy Commissioner surveys Canadians and states "More than eight in 10 respondents (82 percent) opposed giving police and intelligence agencies the power to access e-mail records and other Internet usage data without a warrant from the courts" most of us in law enforcement would back such a statement. But let's be fair, this is not what governments and Canada's law enforcement leaders are proposing.

These same technologies are providing a safe haven for serious criminal activity in Canada – organized crime, sexual predators, gangs, identity theft and terrorism are among the many examples. New technologies allow for old crimes to be committed in new ways, as well as new crimes to develop, including viruses, trojans, worms, hacking, spyware, spam, phishing, identity theft, Internet fraud and money laundering. The fact is that Canada's obsolete legislative scheme was implemented in 1975 during the days of the rotary dial telephone. Modernization of current legislative provisions is urgently required to reflect significant advancements in communications technologies. Without modernization, the current legislation severely challenges police investigations and compromises public safety. Urgent amendments are required to allow the police to lawfully and effectively investigate serious offences. This new law is up-dating laws to reflect new technologies.

We believe new legislation will:

- assist police with the necessary tools to investigate crimes while balancing, if not strengthening the privacy rights for Canadians through the addition of oversight not currently in place.
- help law enforcement investigate and apprehend those who are involved in criminal activity while using new technologies to avoid apprehension due to outdated laws and technology
- allow for timely and consistent access to basic information to assist in investigations of criminal activity and other police duties in serving the public (ie. suicide prevention, notifying next of kin, etc.)

One of the difficulties with regard to the lawful access legislation is presenting it in a fashion that the public can understand as it can be very technical. Our goal is to assist the public to allow them to base their opinion on fact, not rhetoric.

Today`s Environment versus the Proposed legislation:

Currently, there are few set procedures for law enforcement to gain information required to investigate leads relating to criminal activity. Telecommunication service providers (TSP`s) vary widely as to what information will be provided to law enforcement. The following table is used to describe the tightening of rules under Bill C-30 versus the current environment by various applications:

Application	Currently	Through Bill C-30
- Obtaining any content of email, cellular call, etc.	Obtainable only by way of warrant *	Obtainable only by way of warrant *
- Obtaining Basic Subscriber Information in the course of carrying out public safety activities	Ad hoc basis – some TSP's will provide, many others request warrant – Issue is timeliness and consistency in obtaining information – No controls exist on obtaining information	- strict limits on the number of law enforcement officials permitted to request information - those officials to be fully trained - strict procedures for recording, reporting and auditing of such requests - auditing/reporting process includes providing documentation to Minister of Public Safety, Privacy Commissioner, provincial authorities, etc.
- IP address or cellular tracking (monitoring)	- Could only be done through a warrant	- Could only be done through a warrant
- Monitoring Internet Surfing	- Could only be done through a warrant.	- Could only be done through a warrant
- Mechanism to obtain content of email, cellular call, etc.	Obtainable only by way of warrant * Ad hoc basis – TSP's are not required to preserve data. By time law enforcement obtains warrant, content may not be available. Severely handicaps law enforcement and may endangers lives	Obtainable only by way of warrant * - implements production and preservation orders.** - allows law enforcement to request TSP to preserve data while a warrant is being requested (helps ensure data is not lost)

* A warrant is a judicially authorized mechanism to allow law enforcement to gain private information (content or data). There are certain exigent circumstances (ie. life at immediate risk) where law enforcement can obtain this material. This does not change with Bill C-30.

** This legislation introduces production and preservation orders which police can present to a Telecommunication Service Provider. A production order would allow police to gain a limited amount of transmission data for the purpose of ultimately identifying the originating service

provider involved in the transmission of e-mails or other communications and would be granted through a warrant on the basis of "reasonable grounds to suspect." A preservation order request is one that requires the TSP to preserve (i.e. not delete) specific computer or communication data that would assist in an investigation for up to 21 days (90 days for foreign investigations) while police obtain a warrant to be able to view that data.

The Important Facts Around the Legislation:

Access to Actual Data or Content:

Fact: To gain content of electronic communications, a warrant is required. Data or content of transmissions can only be released to law enforcement through a court ordered warrant process. The legislation does not change this. (There are very limited exceptions to this in emergency situations where serious harm must be prevented).

The preservation of data (a 'demand' by a police agency) is a request to a service provider to preserve data for a time period not exceeding 21 days (in order that the police have the opportunity to apply for the requisite warrant to obtain the information). This will necessitate the securing of existing data by the provider and the housing of that data in anticipation of the warrant.

Fact: There is nothing in the bill that asks the provider to specifically monitor the traffic of the individual and report back to the law enforcement agency on the activity of an individual (i.e., this is not a "collection order").

Access to Basic Subscriber Information:

The information which companies would be compelled to release would be: name, address, phone number, email address, Internet protocol address, and the name of the service provider. All of these would involve police providing one identifying set (e.g., IP address and time/date) and the communication service provider providing the matching subscriber information (e.g., customer name). While this information is important to police in all types of investigations, it can be of critical in cases where it is urgent that police locate a caller or originator of information that reasonably causes the police to suspect that someone's safety is at risk. Without this information, the police may not be able to quickly locate and help the person who is in trouble or being victimized.

Fact: Gaining basic subscriber information (names, addresses, phone numbers etc.) would be obtainable pursuant to requests from designated officials in policing agencies through an audited process. This reflects the reality that phone directories do not necessarily exist in the digital world.

The Auditing Process:

Currently, there is no audited process for law enforcement to gain access to basic subscriber information. It may be obtained through a current relationship between a policing service and a TSP or, far too often, is only provided following significant delays. Some TSPs outright deny providing the information without a warrant. *Currently law enforcement agencies are not directly accountable for these requests and for the information that they obtain.*

Fact: Under the proposed legislation, new safeguards will be implemented which actually enhance the privacy of Canadians. These include:

- *strict limits on the number of law enforcement officials permitted to request information*
- *the training of such individuals*
- *strict procedures for recording, reporting and auditing of such requests*
- *the implementation of an auditing/reporting process which includes providing documentation to Public Safety Minsters, Privacy Commissioners, Federal and provincial authorities, etc.*

Compliance by telecoms and ISPs:

Intercepting communications has been cited as an issue because of the cost-prohibitive nature of these upgrades to existing service providers and new entrants into the market.

Fact: *Within this legislation the government recognizes the cost of development for the providers and is prepared to assist in specific circumstances. There is wording that speaks to grandfathering existing providers and the permission of a catch-up period with the possibility of government financial assistance.*

Other:

Tracking of Phones (which have GPS) in the absence of a warrant. Such a possibility currently exists within the Criminal Code (s.487.11), but only for an exigent circumstance (i.e. a kidnapping or extortion). This same section will remain (slightly revised to include a Number Recorder) in the new legislation.

Lawful Access Frequently Asked Questions

Q1

Why do police need warrantless access to basic subscriber information (i.e. subscriber name, address, the existence of services, account information)?

A1

- *Basic subscriber information is often the most basic piece of information needed to progress an investigation, which may later require obtaining a warrant. It is similar to connecting a person's name to their telephone number in an address book. Lack of timely access to such information can, and often does, block investigations. In the case of situation, such as reports of potential suicides, lives can be endangered.*

- *Currently, there are few set procedures for law enforcement to gain information required to investigate leads relating to criminal activity. Telecommunication service providers (TSP`s) vary widely as to what information will be provided to law enforcement. This new legislation will:*

    - *assist police with the necessary tools to investigate crimes while balancing privacy rights for Canadians*
    - *help law enforcement investigate and apprehend those who are involved in criminal activity while using new technologies and avoid apprehension due to outdated laws and technology*
    - *allow for timely and consistent access to basic information to assist in investigations of criminal activity*

- *Towards the end of this document, we have provided a section entitled: "Case Studies: The Utility of Basic Subscriber Information to Law Enforcement" as examples of why police need access to basic subscriber information. As an example of the issue, according to the RCMP's National Child Exploitation Coordination Centre, in 2010, the average response time for a basic subscriber information request was 12 days, and only 72.5% of requests were fulfilled*

- *Other applications:*

    - *Ascertain the address of a witness who has provided their phone number(s).*
    - *To follow up leads in an investigation where they have been provided a phone number and need to:*

    - *know if it belongs to the person it is purported to belong.*
    - *establish an address at which the person resides (presuming the number is a landline because address information on cellular phones is unreliable at best)*
- *To have the information required to obtain a warrant (customer name and address, IP address, phone number, etc.)*
- *As identified above, in emergent cases such as 9-1-1 calls from a cell phone or similar distress communication over the internet. This information may be essential to ensure help is provided to a person as soon as possible.*
- *To expedite investigations involving serious critical matters which require swift police response to apprehend criminals or prevent crime.*
- *To notify next of kin when there has been an accident or homicide*
- *To notify owner when stolen property is recovered.*

Q1 (A)

Why can't police just get a warrant for Basic Subscriber Information?

A1 (A)

- *It may not allow for timely response and potentially jeopardize lives and safety while warrant is being obtained. In many cases, time is of the essence.*
- *It may allow victimization to continue while police attempt to get the warrant*
- *In many cases, law enforcement cannot obtain a warrant without BSI.*
- *How does law enforcement get a warrant for possible suicide threats, next of kin notification on a timely basis?*
- *In the case of missing persons, police often do not have obvious grounds that a crime is involved, nor that it is urgent. A warrant is likely not obtainable, based on the information provided, and the Telecommunication Service Providers (TSP's) are not required to provide BSI . In these cases, the first 24 hours of an investigation is critical.*
- *BSI allows us to investigate expeditiously with minimal intrusion (contact information) into peoples lives*
- *If a warrant was required for each request, police (and Justices) could not keep up with the demand. Further, the complexity of cross-jurisdictional (provincial / national / international) would place a significant workload on policing to obtain warrant for BSI in each location.*
- *Please note: The notion of urgency can be somewhat subjective. With this legislation, it addresses the issue of a uniform policy to gaining such information.*
- *Again, in today's environment, TSP's may be willingly provide BSI information and they may not depending on the practices of individual TSP's. With this legislation, oversight is incorporated which is currently not in place. <u>Law Enforcement is seeking consistency and ensuring that the TSP's are not the ones who randomly decide what we can, or cannot, investigate.</u>*

Q2

Who can ask for basic subscriber information from service providers?

A2

Currently any sworn or civilian police personnel can request this information from a telecommunications company. The new legislation will require the head of a law enforcement agency (i.e. the Chief or Commissioner) to designate a limited number of people within the organization to obtain this information. Mandatory training will be required of all designated officials. Law enforcement will be required to document all requests and disclose them through an audit procedure contained within the bill. The audit procedure includes:

- *strict limits on the number of law enforcement officials permitted to request information*
- *the training of such individuals*
- *strict procedures for recording, reporting and auditing of such requests*
- *the implementation of an auditing/reporting process which includes providing documentation to Public Safety Minsters, Privacy Commissioners, Federal and provincial authorities, etc.*

Q3

What is done with the basic subscriber information obtained by law enforcement personnel from the service providers?

A3

This information is provided to police personnel to aid in investigations and for public safety purposes.

- *There is currently an accepted rule that the information obtained may only be used for the purpose for which it was obtained. There is no body which monitors this at the moment, and no requirement for law enforcement agencies to be accountable for why the information was obtained and how it was used.*

- *The new legislation ensures that:*

    - *law enforcement agencies can account for the reason the information is obtained and also what the information was used for.*
    - *the agency may only use the information for the purpose for which it was obtained.*
    - *the agency organize the information in a fashion that would permit an audit of that information to determine why it was requested and what the information was used for.*

Q4

Do law enforcement agencies actually engage in the interception of private communications without a warrant/judicially approval?

A4

Since 1993, Section 184.4 of the Code has provided that peace officers can intercept private communications without prior judicial authorization, where the peace officer believes on reasonable grounds that: (i) an authorization cannot be obtained with reasonable diligence, given the urgency of the situation; (ii) an interception is immediately necessary to prevent an unlawful act that would cause serious harm to any person or to property; and (iii) either the originator or the intended recipient of the private communication is the person who would perform the harmful act or is the intended victim.

In 2008 the constitutionality of this Section was questioned in a Court case R v. 6 Accused (There is a pending SCC decision). The legislation, as currently written lacks the requirement of reporting to the Attorney General (Provincial) or to Public Safety Canada (Federal) of the use of this measure. Additionally, unlike traditional judicially approved interception, it lacks the requirement of notification to the person(s) intercepted. The former Bill C-50 intended to amend the current legislation to ensure that both these deficits were rectified.

Q5

Will the new legislation actually empower Internet Service Providers (ISPs) to collect information and provide it to law enforcement agencies in the absence of a warrant?

A5

Absolutely not. The law enforcement agency will be permitted the ability to make a "demand" to preserve data for 21 days, which means that the data will be preserved for that time period by the service provider, but the law enforcement agency MUST have a warrant to obtain the data that was preserved by that demand (or to extend the preservation by judicial order for an additional 90 days).

Q6

Won't the new legislation cripple the telecommunications and internet service provider companies financially with all the new requirements to have intercept capability?

A6

This was considered in the drafting of the legislation. Within this legislation the government recognizes the cost of development for the providers and is prepared to assist in specific

circumstances. There is wording that speaks to grandfathering existing providers and the permission of a catch-up period with the possibility of government financial assistance. Note that much more far-reaching laws exist in the United States and Europe where TSP's, (based on competition) have not passed on costs to consumers.

Q7

For those of us who live our lives online and presume that there is some anonymity in that realm, doesn't this legislation provide "the state" the ability to watch our actions and collect information about us on a whim?

A7

This is absolutely not true. This legislation is not designed to do away with the need for a warrant for information currently obtained by way of warrant. This legislation is designed to bring the Criminal Code into this century and this decade and provide for the ability to preserve data that might not otherwise be retained, to allow for law enforcement agencies to apply for the warrants to obtain the information. Crimes involving the use of services and sites available on the internet are on the increase – from child exploitation to identity theft – and law enforcement agencies require the ability to obtain the data required to determine whether the person suspected has committed a crime. This information could only be obtained with the issuance of a warrant by a judge.

The basic subscriber information provision does not give law enforcement the lawful authority to monitor websites for the purpose of creating profiles of individuals, or to track individuals. Under this legislation, police may request the name and address associated with an IP address using a basic subscriber information request.

Requests for information from a telecommunications service provider about the website surfing activity or the real-time whereabouts of an individual would need to be made under production orders, warrants or wiretap authorizations contained in the Criminal Code.

Q8

I heard that telecommunications companies and ISPs will track my location through my phone or internet use and will provide this information to law enforcement. Is this true?

A8

Currently, and as well with the new legislation, such action can only take place with a warrant or in an exigent circumstance telecommunications companies and ISPs will provide this information to law enforcement agencies. A warrant will be required to obtain this information unless a law enforcement agency invokes either s. 487.11, s. 184.4, or s.492.1 of the Criminal Code. Where there have been changes, the new legislation puts new privacy and Charter protections in place and ensures that the service providers must have the capability to provide the information.

Q9

Isn't this legislation simply an attempt by the government and police to position "the state" to have eyes and ears everywhere and have the ability to invade personal privacy at a whim?

A9

The intent of the legislation is to compel service providers to have the capability to intercept private communications under judicial order or in an exigent circumstance. It also stipulates that tombstone information must be provided to law enforcement personal in the absence of a warrant (whereas there is no legislation dictating this or otherwise at the moment) but clarifies the rules that both the police and the service provider must follow. For example, because a service provider would be compelled to disclose, it now places an additional burden on the law enforcement community to provide a clear audit of what the information was requested for and how it was utilized once received (for which there is no current requirement).

Federal Ombudsman for Victims of Crime on the need for Lawful Access

The Office of the Federal Ombudsman for Victims of Crime is an arms-length resource for victims in Canada. The Office was created in 2007 to ensure the federal government meets its responsibilities to victims of crime. Ms. Sue O'Sullivan is Canada's Federal Ombudsman for Victims of Crime. Both her, and her predecessor's have documented the need for Lawful Access.

The Ombudsman has underlined the importance of the issue of child sexual exploitation and the need for lawful access to Parliament. In the report "Every Image, Every Child – Internet-Facilitated Child Sexual Abuse in Canada" the Ombudsman outlines the very serious issues faced by law enforcement. In her testimony before a Senate Standing Committee on Bill C-22 (An Act respecting the mandatory reporting of internet child pornography by persons who provide an internet service) she states:

> *While I am fully supportive of this bill, I must also point out that there is still much more to be done in order to effectively address the issue of Internet-facilitated child sexual abuse. Bill C-22 will not, in and of itself, eradicate child sexual abuse material from being created or shared; nor will it address the challenges that law enforcement will face in pursuing these cases without the necessary authority to compel ISPs to provide basic customer name and address information in order to identify and locate the individuals associated with a particular IP address.*
>
> *Currently in Canada, ISPs are allowed but not obliged to provide customer name and address information without a warrant. Though many companies do cooperate, some can and do refuse to cooperate with law enforcement. In fact, according to the National Child Exploitation Coordination Centre in 2007, 30 per cent to 40 per cent of requests are denied. Without this information, law enforcement may be forced to close a case before a detailed investigation ever begins.*
>
> *When it comes to privacy, the victim's privacy issues also need to take precedence. I do not think there is anything that violates your privacy more as a victim than having your sexual abuse be out there circulating in cyberspace. It is about balance and about respecting the privacy rights of the victims of sexual abuse*

For further information:

- Ms. O'Sullivan testimony February 10, 2011 before the Senate Standing Committee on Legal and Constitutional Affairs on Bill C-22: http://www.parl.gc.ca/Content/SEN/Committee/403/lega/20evb-e.htm?Language=E&Parl=40&Ses=3&comm_id=11
- Every Image, Every Child report: http://www.victimsfirst.gc.ca/res/pub/childp-pjuvenile/cont_01.html
- Every Image, Every Child backgrounder: http://www.victimsfirst.gc.ca/media/news-nouv/bg-di/20090507-1.html
- Every Image, Every Child fast facts/statistics document: http://www.victimsfirst.gc.ca/media/news-nouv/bg-di/20090507-2.html

Case Studies: The Utility of Basic Subscriber Information to Law Enforcement

One of the problems with the current system is that there is no uniformity or reliability as to how/if TSPs respond to requests for basic subscriber information. For instance:

- There is one TSP that only responds to BSI requests on Fridays, regardless of when the requests are submitted
- There is one TSP that only accepts BSI requests via email

The National Child Exploitation Coordination Centre in Ottawa looked at a sample of 1,244 of the basic subscriber information requests they made in 2010. TSPs provided the information in 902 cases (72.5%). However, in 62 cases (5%), the TSPs refused to provide the information without a court order and in 53 cases (4.3%) did not respond to the request. In 227 cases (18.2%) the TSPs did not have the information that authorities requested. These numbers do not include requests made by other units that investigate Internet child exploitation offences across the country.

Furthermore, in 2010, the average response time for these requests was 12 days.

The National Child Exploitation Coordination Centre in Ottawa reported that, in 2007, of the 482 requests they made for basic subscriber information, in 19 cases (3.9%) service providers refused to provide the information without a court order and in 92 cases (19.1%) they did not respond to the request. In 40 cases (8.3%) the service providers did not have the information that was requested. In 2008, the NCECC in Ottawa made 335 requests for basic subscriber information. In 6 cases (1.8%) service providers refused to provide the information without a court order. In 46 cases (13.7%) they did not respond to the request and in 30 cases (9%) the service providers did not have the information that was requested.

Examples of regional disparity regarding telecommunications service providers (TSPs) providing BSI

Sometimes TSPs in specific regions don't respond to requests. Some TSPs in Atlantic Canada will not provide BSI unless they have a warrant.

1) In December 2010, New Brunswick RCMP began to investigate a case of peer-to-peer sharing of child pornography. Police suspected that up to 170 IP addresses were associated with a single individual. These IP addresses belonged to a TSP known for refusing to voluntarily provide subscriber information without a court order so the police applied for one.

   As a result, the basic subscriber information was provided 15 days later and by that time the suspect's Internet activity had stopped. In September 2011, the suspect resumed his online activity and, that time, the TSP provided the basic subscriber information voluntarily. This cooperation allowed the police to act quickly and arrest the suspect at his residence in October 2011. The suspect was charged with possession and distribution of child pornography. Furthermore, police discovered that he was also producing child pornography and he was charged with that crime as well. The suspect also pled guilty to charges, which included the abuse of two young males from New Brunswick. If the police had been able to obtain the

information shortly after the investigation began, the investigation could have proceeded to the arrest stage more rapidly and the suspect's sexual abuse could have been stopped sooner.

Examples where TSPs did not provide police with BSI

2) In 2007, there was an international case involving 88 Canadian Internet Protocol addresses linked to the purchase of child pornography. The police requested the basic subscriber information associated with these addresses. Fifty one requests were answered and police were able to investigate these individuals and in some cases charges were laid. However, 37 requests were unanswered by the service providers. As a result, the identities and location of these suspected pedophiles is still unknown today.

3) In Operation Koala, a major international child pornography case in 2008, Europol provided the RCMP with information relating to 98 Canadian e-mail accounts or Internet Protocol addresses. TSPs were asked to provide the related basic subscriber information about their customers. Many service providers did provide the basic information and it led to the arrest and prosecution of nine Canadians. Regrettably, the identity of 25 Internet Protocol addresses or e-mail accounts could not be established due to the lack of cooperation of some service providers.

4) In Project Penalty, an international child pornography investigation, 47 out of 200 requests for basic subscriber information were refused by the TSPs.

5) In 2007, the RCMP assisted with an international investigation in which suspects located in Canada were attempting to defraud American corporations of approximately $100 million. The investigation required police to find the individuals who were accessing unsecured wireless computer networks in the Toronto area (war driving) to commit these fraudulent activities. The suspects were constantly on the move and police needed the immediate support of the TSPs to determine the location of these networks. However, the service providers would not provide police with the basic subscriber information they needed. Because of the lack of cooperation from the TSPs, it took eight full-time technical investigators five days to finally locate and arrest the suspects. The suspects successfully defrauded victims of $15 million. Had police been provided the information when it was requested, the value of the fraud would have been reduced considerably and police resources would have been used more effectively.

6) A 2006 international criminal investigation involved 78 Canadian Internet Protocol addresses linked to the purchase of child pornography. Requests for basic subscriber information related to those Internet Protocol addresses were submitted to the relevant TSPs and the information was provided for 44 addresses. However, 18 suspects have not been identified since the service providers refused to provide the basic subscriber information without authorities first obtaining a warrant.

7) In 2009, the RCMP in Alberta were notified of a threat made online to carry out a school shooting. Police had the Internet Protocol address and the date and time the threat was made and police requested that the TSP provide the corresponding basic subscriber information. The provider refused to cooperate, saying there was no urgency because the threat to carry out the shooting was six days old. The following day (Friday before a long weekend) police applied for a production order to compel the TSP to provide the information. By the time the production order was issued, the contact at the TSP had left for the weekend and the police had to wait three days before obtaining the information. When the TSP did provide the information, the

police used the information to obtain an additional warrant authorizing the search of a residence. A young person was arrested and remanded pending a mental health evaluation.

Examples of how BSI is useful to locate or identify an individual

8) In 2008, Calgary police were investigating threatening emails that were being sent to a woman from a sender whose identity was concealed. Authorities provided the TSP with the IP address and asked the TSP for the street address from where the emails were sent. The information was provided and, as a result, within one day police were able to identify the individual sending the threatening emails and the investigation was complete. The individual was charged with criminal harassment and the victim got a restraining order against this individual.

9) A child was abducted in British Columbia in 2011. An amber alert was broadcast and, fortunately, the suspect returned the child. However, the suspect was not apprehended and his location remained unknown. Through further investigation, police obtained an IP address associated with the suspect. Police contacted the TSP directly and were advised that it was against policy to provide subscriber information related to an IP address without a Production Order. Police advised the TSP that the suspect had already abducted one child and that other children could possibly be at risk. The TSP decided to provide the information and the suspect was located and apprehended less than 24 hours after police received the information.

10) In 2008, the head of a municipal government in Québec was receiving death threats and harassing calls. In this case, the TSP cooperated and provided basic subscriber information to the police when it was requested and the police were able to locate and arrest the suspect. When the suspect was arrested, the police seized weapons from his house.

11) The Toronto Police Services had at least two cases involving citizens calling the police to advise that they were communicating over the Internet with persons threatening suicide. In both cases, the location of the potential victims was unknown. The police contacted the hosts of the websites and were provided with the IP addresses associated with the suicide threats. The police then contacted the TSPs and were provided with the basic subscriber information without a court order. This allowed the police to locate the distressed persons before they could harm themselves.

Example of how BSI is useful in the early stages of an investigation

12) In 2009, police were called to a homicide in which the victim suffered multiple stab wounds and was left on the street. The police determined that the victim had been involved in an altercation after attending a local pub. One of the victim's friends told police that one of the men suspected of being involved in the murder had called the victim's cell phone prior to the murder. The police looked through the victim's phone and found the cell number of this suspect. The police then provided the suspect's cell phone number to a TSP and obtained the basic subscriber information associated with that number. As a result, the police were able to identify the suspect, and from there more suspects were identified. As information beyond basic subscriber information was required, the police applied for a production order and obtained incriminating text messages.

13) In 2009, a Calgary-based company with 15,000 employees had its server hacked. A large amount of corporate data was stolen including personal records and payroll information. During their investigation, police obtained an IP address from the company, identified the TSP and asked the TSP for the name and address of the customer associated with the address. The TSP refused to voluntarily provide basic subscriber information to the police, so the police obtained a search warrant and the information was provided five days later. The information allowed the police to obtain a search warrant in relation to a residence in Manitoba. Pursuant to the search warrant, police seized the computers of one of the company's previous employees, but the delay that occurred was harmful to the company as the information that was stolen was of great potential use to the company's competitors.

Examples of the need for interception capability

14) In 2008, members of an organized crime group in British Columbia were directing an Agent to commit criminal acts, such as extortion and drug trafficking, through messages on cellular telephones. The service provider did not have the capability to intercept these messages and it took the RCMP six weeks to devise and implement a technical solution. The inability of police to intercept the text messages at a critical point in the investigation meant vital evidence was not collected.

15) The RCMP had installed equipment at a service provider to support an international money laundering and drug investigation. When a separate international terrorism investigation got underway, the police had to redeploy the interception equipment from the money laundering investigation in order to intercept the communications of the primary terrorism target. As a result of having to redeploy the equipment, evidence was lost in the money laundering investigation. If interception capability obligations had been in place, both interceptions could have been performed and evidence would not have been lost.

The Canadian Association of Chiefs of Police has obtained many further examples of the utility of Basic Subscriber Information to Law Enforcement which will be provided in our release to Committee.