Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Willey, Chris

From: Kwavnick, Andrea
Sent: Tuesday, March 20, 2012 10:01 AM
To: Kingsley, Michèle; Paulson, Erika; Spendlove, Jim; [redacted] Joan Butcher (JButcher@justice.gc.ca); Burton, Meredith; Filipps, Lisa; Glazer, David; 'Greg.Scott@bc-cb.gc.ca'; Hawrylak, Maciek; Kousha, Hasti; Lauzon, Adam; Miller, Kevin; PSMediaCentre/CentredesmediasdeSP; Scott, Marcie; Willey, Chris; Wilson, Barbara
Subject: RE: Michael Geist - Halifax Police on Refusals to Provide Subscriber Data: None
Attachments: Demonstrating the Need for BasicSubscriber Information - V5 - February 2012.doc; Demonstrating the Need for BasicSubscriber Information - V5 - Fr - February 2012.doc

Hi Erika,

Attached is the examples document we prepared recently - in English and French. For media requests you may want to highlight some of the stats on the first page:

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
- In 2010, the average response time for BSI requests for the National Child Exploitation Coordination Centre in Ottawa is 13 days.

Thanks
Andrea

-----Original Message-----
From: Kingsley, Michèle
Sent: March-20-12 9:39 AM
To: Paulson, Erika; Spendlove, Jim; [redacted] Joan Butcher (JButcher@justice.gc.ca); Burton, Meredith; Filipps, Lisa; Glazer, David; 'Greg.Scott@bc-cb.gc.ca'; Hawrylak, Maciek; Kousha, Hasti; Kwavnick, Andrea; Lauzon, Adam; Miller, Kevin; PSMediaCentre/CentredesmediasdeSP; Scott, Marcie; Willey, Chris; Wilson, Barbara
Subject: RE: Michael Geist - Halifax Police on Refusals to Provide Subscriber Data: None

Thanks Erika.

Andrea will send an examples document that had been developed the week of tabling.

As background to what Mr. Geist is writing, authorities often do not have evidence of non-compliance due to the nature of the current voluntary system. To illustrate, a policy officer can ask for the information - if he/she doesn't get it, the negative response doesn't get recorded. The voluntary process is verbal. In some areas of the country, police officers don't bother asking for BSI anymore because of years of refusals from TSPs - that doesn't get recorded. In other areas, police obtain it voluntarily due to a cooperative relationship with the TSP - that doesn't get recorded either.

What's being proposed under C-30 would mandate authorities to determine - and audit - exactly what is being requested, what is being provided, and why. The findings of those audits would be reported. The Privacy Commissioner and other privacy oversight bodies could then audit those requests as well.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

If you think turning the above into a response bullet of some kind please let me know.

Merci, Michèle

Michèle Kingsley
Director, Investigative Technologies and Telecommunications Policy | Directrice, Technologies d'enquêtes et politiques des télécommunications National Security Operations | Opérations de la sécurité nationale Public Safety Canada | Sécurité publique Canada
613.949.3181 / michele.kingsley@ps-sp.gc.ca

-----Original Message-----
From: Paulson, Erika
Sent: March-19-12 12:56 PM
To: Spendlove, Jim; [redacted] Joan Butcher (JButcher@justice.gc.ca); Burton, Meredith; Filipps, Lisa; Glazer, David; 'Greg.Scott@bc-cb.gc.ca'; Hawrylak, Maciek; Kingsley, Michèle; Kousha, Hasti; Kwavnick, Andrea; Lauzon, Adam; Maillé, Marie Anick; Miller, Kevin; PSMediaCentre/CentredesmediasdeSP; Scott, Marcie; Willey, Chris; Wilson, Barbara
Subject: FYI: Michael Geist - Halifax Police on Refusals to Provide Subscriber Data: None

FYI - Geist has begun publishing results from his inquiries to local police forces RE non-compliance for voluntary disclosure of BSI by TSPs. According to his recent post, neither Montreal nor Halifax police have evidence of non-compliance. Please find the full article below.

We have a document that provides 5 examples of non-compliance that compromised an investigation, but some are old. Please find it attached. If there are more recent examples/more extensive data on non-compliance for voluntary disclosure, it would prove useful.

Relevant approved MLs are as follows:

- Basic subscriber information is often required at the early stages of investigations and is essential for pursuing investigative leads. The inability to obtain this information in a timely fashion can delay or block important investigations and undermine public safety and security.
- Police also need basic subscriber information for non-investigative purposes. For example, contacting next of kin, returning stolen property or assisting individuals in distress.
- Current federal legislation allows telecommunications service providers to release basic subscriber information to authorities without a warrant. However, they are not required to do so.
- While some service providers do release basic subscriber information to authorities upon request, others fail to provide it in a timely fashion, and others request a warrant. As a result, there is no consistency or predictability across the country when authorities request this basic information and investigations are often delayed or hampered.

Cheers,
Erika Paulson
Tel: 613-993-4415 | BB: [redacted] s.19(1)

*****

FULL ARTICLE:
http://www.michaelgeist.ca/content/view/6382/125/

Halifax Police on Refusals to Provide Subscriber Data: None

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Monday March 19, 2012

Among the government's primary justifications for its lawful access/online surveillance bill (Bill C-30) is that since Internet providers have not been required to disclose subscriber information during an investigation, their assistance is inconsistent. For example, the Public Safety backgrounder on the bill states:

Basic subscriber information is often required at the early stages of investigations or to fulfill general policing duties. This information can already be provided without a warrant under existing legislation, but only on a voluntary basis, which results in inconsistent access and delay.

RCMP data indicates that ISPs complied with nearly 95 percent of requests in 2010, suggesting that non-compliance involves a very small number of cases. I recently filed a series of access to information requests with local police forces to better identify whether they were running into problems. The answer so far is no. The request asked for "a list of all incidents since January 1, 2009 where a request to an Internet service provider for customer name, address, email address, internet protocol address, or IMEI number was refused." The Montreal Police responded that there were no records on point. The Halifax Police was very cooperative and undertook a detailed search. This is notable since Bell Aliant is sometimes identified as an ISP that seeks court orders for disclosure of subscriber information. The Halifax Police report:

A search was conducted using key words such as Bell (2022), ISP (1703), computer (540), Rogers (530), Eastlink (119), Facebook (107), Telus (96), internet (90), Aliant (66), Bell/Aliant (8), Internet Protocol (1) and Kodoo (no results). A review was undertaken and we could not find a refusal.

I'll report on other results as they come in.

Pages 4 to / à 8

are duplicates of

sont des duplicatas des

pages 139 to / à 143

Pages 9 to / à 17

are duplicates of

sont des duplicatas des

pages 144 to / à 152

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

BRIEFING NOTE FOR THE DEPUTY MINISTER

RESPONSIVE ISSUES

s.15(1) - Int'l
s.21(1)(a)

Issue

[redacted] Background information and suggested talking points are provided for your use.

Lawful Access and Encryption

In August 2011, riots erupted throughout a number of UK cities. One of the reasons the violence spread so quickly was that the organizers used certain technologies, notably Blackberry Messenger (BBM), to convene large groups of people to partake in the civil unrest. What makes BBM unique is that almost all messages are encrypted when they leave the sender's phone, and therefore usually cannot be decrypted by authorities.

In the wake of the riots, the UK government and Research in Motion (RIM, the makers of Blackberry) cooperated and RIM committed to meet its obligations to decrypt communications under the *Regulation of Investigatory Powers Act* (RIPA) (2000). Furthermore, on August 25, 2011, Home Secretary Theresa May met with representatives from RIM and other social media companies, including Facebook and Twitter, as well as law enforcement officials, to discuss how law enforcement and social media could use their existing relationships to prevent networks from being used for criminal purposes.

The RIPA is the primary legislation that monitors and regulates the lawful interception of communications in the UK and authorizes the Secretary of State to order Telecommunications Service Providers (TSPs) to implement interception solutions. In addition, TSPs may be compelled to assist with decrypting communications, including providing codes (called keys) in their possession that may be used to decrypt communications.

Canada does not have legislation in place requiring TSPs to have intercept capable equipment. Lawful Access legislation was introduced on November 1, 2010 as the *Investigating and Preventing Criminal Electronic Communications Act* (IPCEC, former Bill C-52), but died on the Order Paper when Parliament was dissolved in March 2011.

The Government's recent election platform included a commitment to combine 12 crime bills and pass them within Parliament's first 100 sitting days. This would include "bills that give law enforcement and national security agencies up to date tools to fight crime in today's high tech telecommunications environment". At this time, however, no clear date for when the legislation will be reintroduced has been established.

Former Bill C-52 had two key components. First, it would have required TSPs to build and maintain intercept capable systems, thereby allowing law enforcement and the Canadian Security Intelligence Service (CSIS) to execute authorizations and judicially authorized

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

warrants to intercept communications in a more timely and consistent manner. Second, it would have compelled TSPs to release basic subscriber information, such as name, address, telephone number, email and IP addresses, to designated police, CSIS and Competition Bureau officials, upon request, and to any requesting police officer in emergencies. Canada's proposed legislation is similar to that of the UK, the United States, and other allied countries.

With regard to encryption, former Bill C-52 would have obligated TSPs to remove any encryption or other treatment that they had applied to the intercepted communications, and would have required them to provide an untreated version of the communication to authorized persons, when possible. However, the legislation would not have required TSPs to decrypt or unscramble a communication if they did not treat the communication in the first place, unlike the UK legislation. Furthermore, the proposed legislation preserved the ability of a TSP to develop encryption technologies that cannot be decrypted, and the ability of a consumer to buy related products.

Refugee Reform (CIC led)

The *Balanced Refugee Reform Act* will come into force on June 29, 2012, and aims at providing protection for those in need and quicker removal of those found not to be in need of protection, thereby deterring abuse and ensuring the integrity of Canada's asylum system and the safety and security of Canadians. It also includes:

- an increase in the annual target for resettled refugees by 2,500 for a total target of 14,500 (i.e., include up to 500 additional government-assisted refugees and 2,000 additional privately sponsored refugees);
- increasing funding under the Resettlement Assistance Program to help refugees from abroad settle in Canada; and
- backlog reduction of pending applications and of individuals pending removal.

As a whole of government initiative, Refugee Reform involves a large number of Departments and agencies as project and program delivery partners, including CIC, the Immigration and Refugee Board (IRB), Public Safety Canada, CBSA, RCMP, CSIS, Justice Canada and the Federal Court.

It should be noted that the original coming into force date of December 1, 2011 was officially delayed to June 29, 2012, to allow more time for implementation and to include a second phase of reforms beyond the original scope.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Hawrylak, Maciek

From: Gernot.Kofler@bc-cb.gc.ca
Sent: January-10-11 4:33 PM
To: Hawrylak, Maciek
Subject: RE: Bureau requests for subscriber information

Thank you!

From: Hawrylak, Maciek [mailto:Maciek.Hawrylak@ps-sp.gc.ca]
Sent: Monday, January 10, 2011 4:30 PM
To: Kofler, Gernot: CB-BC
Cc: Kwavnick, Andrea
Subject: RE: Bureau requests for subscriber information

Gernot,

The CRTC is not included officially as the Act supersedes their tariffed rates and imposes our own. It arrogates the power to decide the fee schedule to PS and the agencies involved in the implementation of the Act.

[redacted] s.21(1)(b)

Maciek

Maciek Hawrylak
National Security Operations Directorate | Direction des Operations de Sécurité Nationale
Public Safety Canada | Sécurité Publique Canada
Tel | Tél : 613-991-6036
Fax | Téléc : 613-991-4669
Maciek.Hawrylak@ps-sp.gc.ca

From: Gernot.Kofler@bc-cb.gc.ca [mailto:Gernot.Kofler@bc-cb.gc.ca]
Sent: January 10, 2011 4:25 PM
To: Hawrylak, Maciek
Subject: Bureau requests for subscriber information

We have been gathering information on the number of requests for subscriber information that the Bureau has made (about 100 a year) and are trying to figure out how many requests we might make with the new Spam legislation. Some figure perhaps 300 but it might be a lot, lot more. More definitive numbers will follow in a couple of days, I hope, as we seek consensus on what the number of requests were and our best estimates on what they might be in the future. Our people are visiting with the Americans and will obtain info on the number of requests they make under their CanSpam legislation, giving us some benchmark for what we might expect.

Still, even if the number of requests reaches thousands (no-one is suggesting tens of thousands), the overall cost of fees will be modest, as they are for CSIS and the RCMP.

Do you know why the CRTC is not part of the Working Group's discussion of subscriber information fees?

Pages 21 to / à 22

are withheld pursuant to section

sont retenues en vertu de l'article

69(1)(g) re (f)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 23 to / à 37

are withheld pursuant to section

sont retenues en vertu de l'article

69(1)(g) re (f)

of the Access to Information

de la Loi sur l'accès à l'information

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Hawrylak, Maciek

From: Gernot.Kofler@bc-cb.gc.ca
Sent: January-31-11 2:27 PM
To: Hawrylak, Maciek
Cc: Douglas.Pentland@bc-cb.gc.ca; William.Bradley@bc-cb.gc.ca; Dominy.McClellan@bc-cb.gc.ca; Kwavnick, Andrea
Subject: RE: Estimate of Bureau look-up requests for subscriber information under anti-spam legislation

We have discussed the estimates again, and although this would only be a best guess at this time, we can live with the general numbers being put forward. Therefore, the Competition Bureau's best estimate of the usage of the subscriber regime under IPCEC will be approximately 3,000 requests per annum (1,000 by telephone number, 2,000 by/for IP address).

From: Hawrylak, Maciek [mailto:Maciek.Hawrylak@ps-sp.gc.ca]
Sent: Friday, January 28, 2011 11:38 AM
To: Kofler, Gernot: CB-BC
Cc: Pentland, Douglas: CB-BC; Bradley, William: CB-BC; McClellan, Dominy: CB-BC; Kwavnick, Andrea
Subject: RE: Estimate of Bureau look-up requests for subscriber information under anti-spam legislation

Gernot,

Many thanks, this is helpful information. Can I just summarize what I understand to be your numbers, just to be sure I understand it correctly?:

1. CB currently makes 1,000 subscriber requests per year, in which it provides the telephone number to the TSP and the TSP returns the name and address. This number is expected to remain the same.
2. CB expects to perform a significant number of searches for/by IP address under IPCEC. For argument's sake, I will use the number 3,000.

Therefore, CB's total expected usage of the subscriber regime under IPCEC will be 4,000 per annum (1,000 by telephone number, 3,000 by/for IP address). Grateful you confirm if these figures are reasonable estimates.

Best,
Maciek

Maciek Hawrylak
National Security Operations Directorate | Direction des Operations de Sécurité Nationale
Public Safety Canada | Sécurité Publique Canada
Tel | Tél : 613-991-6036
Fax | Téléc : 613-991-4669
Maciek.Hawrylak@ps-sp.gc.ca

From: Gernot.Kofler@bc-cb.gc.ca [mailto:Gernot.Kofler@bc-cb.gc.ca]
Sent: January 28, 2011 11:30 AM
To: Hawrylak, Maciek
Cc: Douglas.Pentland@bc-cb.gc.ca; William.Bradley@bc-cb.gc.ca; Dominy.McClellan@bc-cb.gc.ca
Subject: Estimate of Bureau look-up requests for subscriber information under anti-spam legislation

> Hello Maciek. A short while ago, I indicated to you the parameters of the number of subscriber look-up requests that the Competition Bureau anticipates making under the new anti-spam legislation. I had indicated some thousands, certainly below ten thousand. Our considered estimate remains largely the same.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Currently, the Bureau is making 1,000 telephone type subscriber requests per year. These include Bureau requests for subscriber information by our Resource Centre and for our work related to the Canadian Anti-Fraud Centre. http://www.phonebusters.com/english/cafc_aboutus.html

We expect a significantly higher number of computer type subscriber information, like IP addresses under the Spam legislation, but we do not know by how much. We are thinking the number will rise by a few thousand.

Pages 40 to / à 45

are withheld pursuant to section

sont retenues en vertu de l'article

69(1)(g) re (f)

of the Access to Information

de la Loi sur l'accès à l'information

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Scott, Marcie

From: Hawrylak, Maciek
Sent: February-28-11 4:32 PM
To: Chayer, Marie-Helene
Subject: Report on 12th Privacy and Security Conference, 17-18 February
Attachments: Summary - 12th Privacy & Security Conference v1.doc

Marie-Helene,

Below and attached you will find my report from the 12th Privacy and Security Conference that took place in Victoria 17-18 February. I'm happy to discuss further if any point intrigues you.

Maciek

Summary: The 12th annual Privacy and Security Conference was held in Victoria, BC, from 17-18 February 2011. **Lawful access** and **PIPEDA** were discussed during one panel session, which included notable privacy advocates, industry representatives, and government figures such as **Dr. Michael Geist** (University of Ottawa), **Suzanne Morin** (Bell Canada), and **Robin Gould-Soil** (Office of the Privacy Commissioner), among others. The panel concluded that lawful access was **controversial** due to **insufficient oversight**, especially of the basic subscriber information regime, and a **failure to demonstrate a need** on the part of authorities. Other panel sessions of interest but not directly related to lawful access included a **statistical review of data and identity theft**, and a general overview of the **history and meaning of privacy** by noted privacy academic **Jeff Jarvis** (City University of New York).

2. **Lawful access and PIPEDA (C-29)**: Lawful access and PIPEDA were discussed during a frank discussion entitled "Information Regulation – The Federal Approach". Moderated by Jacob Glick (Canada Policy Counsel, Google), the panel included prominent privacy advocates, industry representatives, lawyers, and government representatives, namely Dr. Geist (Canada Research Chair of Internet and E-commerce Law, University of Ottawa), Suzanne Morin (Assistant General Counsel & Privacy Chief, Bell Canada), Robin Gould-Soil (Director, PIPEDA Investigations, Office of Privacy Commissioner of Canada), and Shaun Brown (Counsel, Law Office of Kris Klein). The panel was in agreement that Bill C-52 was "controversial", and especially the basic subscriber information component.

3. **Ms. Morin** pointed to the "significant capital and operating cost" associated with interception as a major industry concern, and also claimed that the list of identifiers related to BSI is "longer than most are comfortable with." **Dr. Geist** was indignant that the BSI regime would introduce mandatory disclosure without court oversight, recalling former Minister Day's pledge to require warrants. Geist remarked that AT&T in the US had been found to be disclosing information unnecessarily to government, concluding that if we build the infrastructure without oversight, abuse is inevitable. He also strongly criticized government for having failed to make the case for C-52, noting that the Toronto 18 had been caught using the existing system. According to Geist, the onus is on government to prove that C-52 is necessary. **Ms. Gould-Soil** noted that lawful access was one of the OPC's four priorities, and that the Office shared Geist's belief that necessity had not been demonstrated. Gould-Soil also raised questions regarding proportionality and clear accountability, and noted that the OPC would make use of the external auditing provisions of C-52, declaring that the Office "was already getting ready to go in if the law is passed." **Mr. Brown** noted that Charter challenges of the BSI regime were, in his opinion, likely.

4. The panel also demonstrated some inconsistency in terms of their understanding of lawful access. Mr. Brown, for example, declared that the BSI regime would allow authorities to track online behaviour, while Dr. Geist claimed that C-52 would result in "a wholesale change in the how the Internet works" and also warned that it would require deep packet inspection (a claim debunked by Ms. Morin).

5. There was a brief discussion on **C-29**, with Ms. Morin and Dr. Geist both querying Ms. Gould-Soil as to whether the OPC had sufficiently availed itself to date of the tools at its disposal. Morin believed that the OPC should be testing its power to 'name names', see if this is challenged in the courts, and let the courts assess damages (for which they have abundant expertise). Gould-Soil retorted that they must meet a high threshold of reasonable grounds before the OPC is able to name names. Geist and Morin both concluded that OPC should be naming the names of organizations when there is a high probability of breach. If they fail in court, the pair argued, it will simply clarify what is considered 'reasonable grounds'.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

6. **PIPEDA after 10 years**: Dr. Geist also conducted a separate keynote glancing back at PIPEDA over the past decade, and looking forward. He listed the naming of names, penalty powers, government accountability, jurisdictional issues, and Constitutional challenges (recent cases of Facebook, CIBC, Canada.com) as current issues. Looking forward, Geist saw enforcement (order making powers), transparency (naming names), a shift from information access to proactive disclosure (à la Google Dashboard), court challenges, opt-in versus opt-out issues, and distributed privacy regulation (e.g. CRTC, Competition Bureau, provincial regulators) as being the top items on the Office's agenda for the next five years. Geist concluded by noting that PIPEDA had reached the limits of competency in some senses, remarking that anti-spam, identity theft, do-not-call, lawful access, and other pressing privacy issues have been handled outside of the PIPEDA legislative framework. He believed that it would be interesting to watch if privacy legislation continued to be balkanized, splintered according to the issue, or whether PIPEDA would reassert its standing as the 'central' privacy protection vehicle at the federal level.

7. **Lawful access and access to information abroad**: Two other panelists made brief but interesting remarks about lawful access and access to information in the United States and Mexico. **Nicole Ozer**, Technology and Civil Liberties Policy Director, **American Civil Liberties Union** (ACLU), noted that the ACLU is pressing for the Obama Administration to require that a warrant be sought to collect location information under the Electronic Communications Privacy Act (1986). She noted that Sprint had fielded 8 million requests for location information from LEAs in 2010. **Sigrid Arzt**, Commissioner of the **Federal Institute for Access to Public Information and Data Protection** (IFAI), Mexico, delivered a luncheon keynote in which she described Mexico's centralized, online access to information portal, Infomex. Under Infomex (https://www.infomex.org.mx), members of the public create a user ID and can enter search queries electronically. These queries are then forwarded to the relevant federal agency(ies), which responds to the request within the 20 days allowed by law. Once the answer is provided, both the question and the answer are posted to the website and are searchable by keyword. All 236 federal agencies form part of Infomex, and the average response time is 13 days. Highlighting the differences between Canada and Mexico, Arzt also noted that 23 million children under 17 in Mexico have had biometric information (fingerprints, etc.) recorded for identification purposes.

8. **Data theft and crime trends**: Several other speakers presented interesting analyses of trends in data and identity theft. **Sean Doherty**, Chief Technology Officer, Enterprise Security Group, **Symantec**, noted that cybercriminals earned about $700 billion last year, which eclipsed the value of the global drug trade (roughly $500 billion). The growth in cybercriminality is about 10% per year. Ninety percent of organized crime targets corporate software rather than individuals, and about 48% of breaches are inside jobs (according to Telus, roughly 33% in Canada). Doherty noted that the explosion of information created has made protection increasingly difficult – the amount of data created grew 600% from 2005-2010 to reach 988 exabytes. **Ritchie Leslie**, Director Western Canada, **TELUS** Security Solutions, noted that data breaches in Canada have grown 29% from 2009, but that breach costs are down 78% since we are able to locate them more quickly. According to Leslie, 60% of malware that passes through the Telus lab is designed to steal identities. Interestingly, he noted that organizations that block social media experienced marginally more breaches than those that allowed them.

9. **History and meaning of privacy**: **Jeff Jarvis**, Associate Professor and Director, Interactive Journalism, **City University of New York's** Graduate School of Journalism, delivered the keynote lecture on the first day, revolving around the interconnections and distinctions between 'privacy and publicness'. For Jarvis, the history of privacy is shaped by the Gutenberg Parenthesis, which notes that prior to the invention of the printing press, communications were oral and impermanent, with no attribution. Communications were radically transformed after Gutenberg: they were serial, linear, permanent, attributable. Finally, the Internet is reversing that trend back to the oral tradition, making things impersonal, but attributable. All thoughts can be published, and the author is known, but the styles range from 'streams of consciousness' to fully-formed theses. The use of the term privacy is rather new, with the first known use of it in the US in 1890, referring to a picture taken of the President with the first Kodak camera. For Jarvis, privacy is "the responsibility of knowing"; it is the decision to transfer that responsibility to another person. Jarvis then ventured into his view on government transparency, noting that government should be open by default, and secret only by necessity. The concept of freedom of information, according to Jarvis, should be turned on its head: government should show why it should keep information from citizens, rather than guard it and only release it when requested.

10. **Comment**: Lawful access panelists targeted the basic subscriber regime much more forcefully than the interception component, registering that the lack of judicial oversight meant that abuse was a matter of 'when', not 'if'. Moreover, at least three of the four panelists felt that the government has not sufficiently made a transparent case of the need for C-52, perhaps signaling an area where Public Safety could redouble its efforts. The Bell representative focused primarily on cost, while the OPC panelist made it clear that the Office would be following this Bill closely and was prepared to act swiftly using its audit powers. The panelists were not shy in showing their displeasure with C-52, but sanguinely remarked that it did not seem to have much government support behind it. The other sessions of the conference demonstrated the growing impact of cybercrime, and the tension between privacy and the public space – with

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

our desire for privacy on the one hand and the need to connect and share information through social media and the like on the other. It was a good conference – though perhaps not immediately related to investigative technologies and telecommunications policy – that attracted a series of interesting and influential speakers, and it may be worthwhile that different representatives from Public Safety attend future meetings to keep current on academic and industry thought in these domains.

Drafted: NSOD/Hawrylak
Date: 28 February 2011

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Notes from 12th Privacy and Security Conference
Victoria, BC, 17-18 February 2011

Summary: The 12th annual Privacy and Security Conference was held in Victoria, BC, from 17-18 February 2011. **Lawful access** and **PIPEDA** were discussed during one panel session, which included notable privacy advocates, industry representatives, and government figures such as **Dr. Michael Geist** (University of Ottawa), **Suzanne Morin** (Bell Canada), and **Robin Gould-Soil** (Office of the Privacy Commissioner), among others. The panel concluded that lawful access was **controversial** due to **insufficient oversight**, especially of the basic subscriber information regime, and a **failure to demonstrate a need** on the part of authorities. Other panel sessions of interest but not directly related to lawful access included a **statistical review of data and identity theft**, and a general overview of the **history and meaning of privacy** by noted privacy academic **Jeff Jarvis** (City University of New York).

2. **Lawful access and PIPEDA (C-29)**: Lawful access and PIPEDA were discussed during a frank discussion entitled "Information Regulation – The Federal Approach". Moderated by Jacob Glick (Canada Policy Counsel, Google), the panel included prominent privacy advocates, industry representatives, lawyers, and government representatives, namely Dr. Geist (Canada Research Chair of Internet and E-commerce Law, University of Ottawa), Suzanne Morin (Assistant General Counsel & Privacy Chief, Bell Canada), Robin Gould-Soil (Director, PIPEDA Investigations, Office of Privacy Commissioner of Canada), and Shaun Brown (Counsel, Law Office of Kris Klein). The panel was in agreement that Bill C-52 was "controversial", and especially the basic subscriber information component.

3. **Ms. Morin** pointed to the "significant capital and operating cost" associated with interception as a major industry concern, and also claimed that the list of identifiers related to BSI is "longer than most are comfortable with." **Dr. Geist** was indignant that the BSI regime would introduce mandatory disclosure without court oversight, recalling former Minister Day's pledge to require warrants. Geist remarked that AT&T in the US had been found to be disclosing information unnecessarily to government, concluding that if we build the infrastructure without oversight, abuse is inevitable. He also strongly criticized government for having failed to make the case for C-52, noting that the Toronto 18 had been caught using the existing system. According to Geist, the onus is on government to prove that C-52 is necessary. **Ms. Gould-Soil** noted that lawful access was one of the OPC's four priorities, and that the Office shared Geist's belief that necessity had not been demonstrated. Gould-Soil also raised questions regarding proportionality and clear accountability, and noted that the OPC would make use of the external auditing provisions of C-52, declaring that the Office "was already getting ready to go in if the law is passed." **Mr. Brown** noted that Charter challenges of the BSI regime were, in his opinion, likely.

4. The panel also demonstrated some inconsistency in terms of their understanding of lawful access. Mr. Brown, for example, declared that the BSI regime would allow authorities to track online behaviour, while Dr. Geist claimed that C-52 would result in "a wholesale change in the how the Internet works" and also warned that it would require deep packet inspection (a claim debunked by Ms. Morin).

5. There was a brief discussion on **C-29**, with Ms. Morin and Dr. Geist both querying Ms. Gould-Soil as to whether the OPC had sufficiently availed itself to date of the tools at its disposal. Morin believed that the OPC should be testing its power to 'name names', see if this is challenged in the courts, and let the courts assess damages (for which they have abundant expertise). Gould-Soil retorted that they must meet a high threshold of reasonable grounds before the OPC is able to name names. Geist and Morin both concluded that OPC should be naming the names of organizations when there is a high probability of breach. If they fail in court, the pair argued, it will simply clarify what is considered 'reasonable grounds'.

6. **PIPEDA after 10 years**: Dr. Geist also conducted a separate keynote glancing back at PIPEDA over the past decade, and looking forward. He listed the naming of names, penalty powers, government accountability, jurisdictional issues, and Constitutional challenges (recent cases of Facebook, CIBC, Canada.com) as current issues. Looking forward, Geist saw enforcement (order making powers), transparency (naming names), a shift from information access to proactive disclosure (à la Google Dashboard), court challenges, opt-in versus opt-out issues, and distributed privacy regulation (e.g. CRTC,

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Competition Bureau, provincial regulators) as being the top items on the Office's agenda for the next five years. Geist concluded by noting that PIPEDA had reached the limits of competency in some senses, remarking that anti-spam, identity theft, do-not-call, lawful access, and other pressing privacy issues have been handled outside of the PIPEDA legislative framework. He believed that it would be interesting to watch if privacy legislation continued to be balkanized, splintered according to the issue, or whether PIPEDA would reassert its standing as the 'central' privacy protection vehicle at the federal level.

7. **Lawful access and access to information abroad**: Two other panelists made brief but interesting remarks about lawful access and access to information in the United States and Mexico. **Nicole Ozer**, Technology and Civil Liberties Policy Director, **American Civil Liberties Union** (ACLU), noted that the ACLU is pressing for the Obama Administration to require that a warrant be sought to collect location information under the Electronic Communications Privacy Act (1986). She noted that Sprint had fielded 8 million requests for location information from LEAs in 2010. **Sigrid Arzt**, Commissioner of the **Federal Institute for Access to Public Information and Data Protection** (IFAI), Mexico, delivered a luncheon keynote in which she described Mexico's centralized, online access to information portal, Infomex. Under Infomex (https://www.infomex.org.mx), members of the public create a user ID and can enter search queries electronically. These queries are then forwarded to the relevant federal agency(ies), which responds to the request within the 20 days allowed by law. Once the answer is provided, both the question and the answer are posted to the website and are searchable by keyword. All 236 federal agencies form part of Infomex, and the average response time is 13 days. Highlighting the differences between Canada and Mexico, Arzt also noted that 23 million children under 17 in Mexico have had biometric information (fingerprints, etc.) recorded for identification purposes.

8. **Data theft and crime trends**: Several other speakers presented interesting analyses of trends in data and identity theft. **Sean Doherty**, Chief Technology Officer, Enterprise Security Group, **Symantec**, noted that cybercriminals earned about $700 billion last year, which eclipsed the value of the global drug trade (roughly $500 billion). The growth in cybercriminality is about 10% per year. Ninety percent of organized crime targets corporate software rather than individuals, and about 48% of breaches are inside jobs (according to Telus, roughly 33% in Canada). Doherty noted that the explosion of information created has made protection increasingly difficult – the amount of data created grew 600% from 2005-2010 to reach 988 exabytes. **Ritchie Leslie**, Director Western Canada, **TELUS** Security Solutions, noted that data breaches in Canada have grown 29% from 2009, but that breach costs are down 78% since we are able to locate them more quickly. According to Leslie, 60% of malware that passes through the Telus lab is designed to steal identities. Interestingly, he noted that organizations that block social media experienced marginally more breaches than those that allowed them.

9. **History and meaning of privacy**: **Jeff Jarvis**, Associate Professor and Director, Interactive Journalism, **City University of New York's** Graduate School of Journalism, delivered the keynote lecture on the first day, revolving around the interconnections and distinctions between 'privacy and publicness'. For Jarvis, the history of privacy is shaped by the Gutenberg Parenthesis, which notes that prior to the invention of the printing press, communications were oral and impermanent, with no attribution. Communications were radically transformed after Gutenberg: they were serial, linear, permanent, attributable. Finally, the Internet is reversing that trend back to the oral tradition, making things impersonal, but attributable. All thoughts can be published, and the author is known, but the styles range from 'streams of consciousness' to fully-formed theses. The use of the term privacy is rather new, with the first known use of it in the US in 1890, referring to a picture taken of the President with the first Kodak camera. For Jarvis, privacy is "the responsibility of knowing"; it is the decision to transfer that responsibility to another person. Jarvis then ventured into his view on government transparency, noting that government should be open by default, and secret only by necessity. The concept of freedom of information, according to Jarvis, should be turned on its head: government should show why it should keep information from citizens, rather than guard it and only release it when requested.

10. **Comment**: Lawful access panelists targeted the basic subscriber regime much more forcefully than the interception component, registering that the lack of judicial oversight meant that abuse was a matter of 'when', not 'if'. Moreover, at least three of the four panelists felt that the government has not sufficiently made a transparent case of the need for C-52, perhaps signaling an area where Public Safety

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

could redouble its efforts. The Bell representative focused primarily on cost, while the OPC panelist made it clear that the Office would be following this Bill closely and was prepared to act swiftly using its audit powers. The panelists were not shy in showing their displeasure with C-52, but sanguinely remarked that it did not seem to have much government support behind it. The other sessions of the conference demonstrated the growing impact of cybercrime, and the tension between privacy and the public space – with our desire for privacy on the one hand and the need to connect and share information through social media and the like on the other. It was a good conference – though perhaps not immediately related to investigative technologies and telecommunications policy – that attracted a series of interesting and influential speakers, and it may be worthwhile that different representatives from Public Safety attend future meetings to keep current on academic and industry thought in these domains.

Drafted: NSOD/Hawrylak
Date: 28 February 2011

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Scott, Marcie

From: Moshonas, Jennifer
Sent: April-01-11 9:42 AM
To: 'Ali Noorbhai'; 'Nisrine Slaymane'; 'Antonio Utano'
Cc: Thompson, Julie
Subject: FW: Teleconference with Sasktel, Industry Canada, Public Safety Canada and RCMP
Attachments: regina & saskatoon cell numbers.XLS

Good morning,

Hope you are well.

Quick question that I am hoping you can assist us with.

My DG is briefing up today on the issue of Sasktel specifically, but more broadly on the current limited application of the SGES. We would like to know what types of investigations these limitation are affecting? Just high level categories would be great if you can e.g. National Security, Organized Crime etc. to include in the messaging to the ADM/DM.

Many thanks,

Jen

Jennifer Moshonas
Senior Policy Analyst / Analyste principale de politiques
National Security Operations Directorate / Direction des Operations de Sécurité Nationale
National Security Technologies/Technologies de Sécurité Nationale
Public Safety Canada / Sécurité Publique Canada
Tel: (613) 998-8035
Email: jennifer.moshonas@ps.gc.ca

From: Ron Sharpe [mailto:Ron.SHARPE@rcmp-grc.gc.ca]
Sent: December 10, 2010 10:09 AM
To: Thompson, Julie; Ali Noorbhai; Ed Pasetka
Cc: Antonio Utano; Jean-Yves Marsolais; Les Gjertsen; Mark Flynn; Nisrine Slaymane; Val Boyetchko
Subject: Re: Teleconference with Sasktel, Industry Canada, Public Safety Canada and RCMP

Hello,

Since our teleconference with SaskTel, we have put together some numbers of intercepts done on Bell, Virgin, and Telus customers in both Regina and Saskatoon for the years 2009 and 2010 (45). See attached spreadsheet for breakdown.

I will be providing these numbers to our SaskTel security contact here in Regina, [redacted] s.19(1)

Ron Sharpe, C/M
Technologist
"F" Division Special 'I' Section
Regina, SK
ph. (306) 780-6859

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

fax (306) 780-8878

>>> Ali Noorbhai 12/9/2010 9:16 AM >>>
Hi, **s.21(1)(b)**

I was at a Bell meeting yesterday after the Sasktel call and [redacted]

I did give Bell manager a heads-up that Bell may be called upon to attend the next conf call as was discussed on the call.

Ali

>>>
From: "Thompson, Julie" <Julie.Thompson@ps-sp.gc.ca>
To:'Ed Pasetka' <Ed.Pasetka@rcmp-grc.gc.ca>, Ali Noorbhai <Ali.Noorbhai@rcmp-grc.gc.ca>
CC: Jean-Yves Marsolais <Jean.Yves.Marsolais@rcmp-grc.gc.ca>, Les Gjertsen <Les.Gjertsen@rcmp-grc.gc.ca>, Nisrine Slaymane <nisrine.slaymane@rcmp-grc.gc.ca>, Ron Sharpe <Ron.SHARPE@rcmp-grc.gc.ca>, Val Boyetchko <Val.Boyetchko@rcmp-grc.gc.ca>
Date: 12/3/2010 8:42 AM
Subject: Teleconference with Sasktel, Industry Canada, Public Safety Canadaand RCMP

Good morning,

The conference call with Sasktel has been scheduled for December 8, 2010, 9:00-11:00 am Ottawa time.

The coordinates for the conference call are as follows:
Teleconference dial in numbers:
Outside of Ottawa: 1-877-413-4781
Ottawa: 613-960-7510
Participants: [redacted]
President: [redacted] **s.16(2)(c)**
Please confirm your attendence with me via e-mail.

Regards,
Julie

Julie Thompson
Policy Analyst/Analyste en politiques
National Security Technologies/Technologies de Sécurité Nationale
Public Safety Canada/Sécurité Publique Canada
tel: 613.998.7893
julie.thompson@ps-sp.gc.ca<mailto:julie.thompson@ps-sp.gc.ca>

From: Ed Pasetka [mailto:Ed.Pasetka@rcmp-grc.gc.ca]
Sent: December 1, 2010 11:51 AM
To: Thompson, Julie; Ali Noorbhai
Cc: Jean-Yves Marsolais; Les Gjertsen; Nisrine Slaymane; Ron Sharpe; Val Boyetchko
Subject: RE: Teleconference with Sasktel, Industry Canada, Public SafetyCanadaand RCMP

Julie

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Just a update on SaskTel SMS issue.

Is there any anticipated time frame for the resolution to our SMS Issue.

Thanks in Advance

E.J. PASETKA Cpl.
Regina Spl "I"

>>> "Thompson, Julie" <Julie.Thompson@ps-sp.gc.ca> 11/17/2010 8:38 AM >>>
Good morning,
I just want to let you know that, unfortunately, one of SaskTel's engineer was unavailable for the conference call this morning, therefore it has been cancelled. I am still working with Industry Canada to find an appropriate time that suits all parties.

I will keep you informed.

Julie

Julie Thompson
Policy Analyst/Analyste en politiques
National Security Technologies/Technologies de Sécurité Nationale
Public Safety Canada/Sécurité Publique Canada
tel: 613.998.7893
julie.thompson@ps-sp.gc.ca<mailto:julie.thompson@ps-sp.gc.ca>

From: Ed Pasetka [mailto:Ed.Pasetka@rcmp-grc.gc.ca]
Sent: November 9, 2010 10:57 AM
To: Thompson, Julie
Cc: Jean-Yves Marsolais; Les Gjertsen; Ron Sharpe
Subject: Re: Teleconference with Sasktel, Industry Canada, Public Safety Canadaand RCMP

Julie

I will be available for call, I would like to have our Tech's C/M Ron SHARPE and C/M Les Gjertsen added to the conference call.

Thanks

Ed PASETKA Cpl.
Regina Spl "I" Section
(306) 780-6858

>>> "Thompson, Julie" <Julie.Thompson@ps-sp.gc.ca> 11/9/2010 7:54 AM >>>
Good morning,
s.19(1)
Industry Canada has contacted [redacted] to arrange a teleconference with representatives from SaskTel, Industry Canada, Public Safety Canada and the RCMP, to discuss the issue of lawful intercept as it pertains to IC's letter of August 10, 2010 (attached) and SaskTel's reply of August 16, 2010 (attached).

Please let me know your availability for the morning of November 17, 2010 and if I should be inviting anyone else from

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

your organization.

Thank you
Julie

Julie Thompson
Policy Analyst/Analyste en politiques
National Security Technologies/Technologies de Sécurité Nationale
Public Safety Canada/Sécurité Publique Canada
tel: 613.998.7893
julie.thompson@ps-sp.gc.ca<mailto:julie.thompson@ps-sp.gc.ca>

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Pages 57 to / à 69

are withheld pursuant to section

sont retenues en vertu de l'article

69(1)(g) re (f)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 70 to / à 72

are withheld pursuant to section

sont retenues en vertu de l'article

69(1)(g) re (f)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 73 to / à 77

are withheld pursuant to section

sont retenues en vertu de l'article

69(1)(g) re (f)

of the Access to Information

de la Loi sur l'accès à l'information

Page 78

is a duplicate of

est un duplicata de la

page 104

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Kwavnick, Andrea

From: Bernard Tremblay <Bernard.Tremblay@rcmp-grc.gc.ca>
Sent: October-12-11 10:41 AM
To: Hawrylak, Maciek
Cc: Kwavnick, Andrea; Kingsley, Michèle; Helene Van Dyke
Subject: Presentation to Privacy Commissioner - 2009
Attachments: LA&CNA RCMP Presentation to Privacy Comm 8July2009.ppt

Hi Maciek,

Here is the presentation we referred to at last Friday's meeting.

Bernie

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RCMP

ROYAL CANADIAN MOUNTED POLICE

Lawful Access and Policing

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RCMP
ROYAL CANADIAN MOUNTED POLICE

Background

Lawful access consists of legislative measures:

- ✓ for lawful interception infrastructure obligations; and
- ✓ for customer name and address (CNA) information.

- Such measures are essential in the prevention, investigation and prosecution of serious offences, including organized crime, and threats to national security.

- Such measures are subject to and respect the *Canadian Charter of Rights and Freedoms*

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RCMP
ROYAL CANADIAN MOUNTED POLICE

Background

- **Lawful Access measures are an essential component of the Government's Public Safety Agenda, National Security Policy and Anti-Terrorism Plan, as well as the Speech from the Throne commitments to combat child pornography and hate crimes.**
- **Canada and Japan are the only G-8 countries that do not have intercept capability legislation.**
- **New legislation requiring telecommunications service providers (TSPs) to develop and maintain intercept capable systems would not grant new surveillance powers to police or national security agencies.**
- **Police and national security agencies derive their lawful authority to intercept communications (e.g. wire tap) from other federal laws.**

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RCMP

ROYAL CANADIAN MOUNTED POLICE

Lawful Interception Infrastructure Obligations

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RCMP
ROYAL CANADIAN MOUNTED POLICE

The Need for Legislated Infrastructure Obligations

- **Rapidly improving telecommunications technologies clearly benefit Canadian society in many ways, but their illicit use creates significant public safety challenges.**

- **Technologies such as the Internet, cellular telephones, smart phones and encryption increasingly challenge law enforcement and national security agencies' lawful interception capabilities.**

- **Criminals and terrorists are using these technologies to shield their activities from detection and as tools to facilitate the commission of serious offenses.**

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RCMP
ROYAL CANADIAN MOUNTED POLICE

The Need for Legislated Infrastructure Obligations

- **Since the mid-1990s, deregulation, technological evolution, and user demand of the telecommunications industry has led to the creation of over 400 TSPs in Canada and new telecom services, such as VoIP (voice over IP) services.**
- **The telecommunications environment, in which law enforcement and national security agencies must carry out their investigations, now is constantly in flux.**
- **Federal laws allow courts to authorize law enforcement and national security agencies to intercept communications, but there are no laws in Canada that require telecommunications service providers to develop and maintain systems capable of being intercepted.**
- **As a result, law enforcement and national security agencies are spending considerable time and money developing technical solutions.**
- **Also, investigations of serious crimes are delayed and public safety is compromised.**

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RCMP
ROYAL CANADIAN MOUNTED POLICE

Customer Name and Address (CNA) Information

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RCMP ROYAL CANADIAN MOUNTED POLICE

Problem with the Status Quo is Reliance on Voluntary Cooperation

- **Requests for voluntary release of customer name and address information are currently made:**
  - **Formally – e.g., by Law Enforcement Request (LER) forms that police and certain ISPs have agreed to use for child sexual exploitation cases**
  - **Informally – e.g. by verbal or written request to a TSP for any other law enforcement purpose (general policing or investigative duties)**
- **RCMP's National Child Exploitation Coordination Centre maintains data on LER requests, but for all the other types of investigation we do not do so**
- **Other police services don't keep a running total or other data about informal requests to TSPs for voluntary disclosure of CNA**
- **Statutory requirements for requesting and protecting CNA would clarify for TSPs and law enforcement agencies what Parliament and the public expects of them**

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RCMP
ROYAL CANADIAN MOUNTED POLICE

Need For Legislative Access to TSPs' CNA Info

- **Police require CNA for their daily work. Police need to receive CNA on request (without a warrant process) for:**
  - **General policing duties (e.g., locating people in crisis, such as suicidal people, and finding and notifying next of kin)**
  - **Greater efficiency & effectiveness (i.e., CNA is preliminary information, gathered at the early stages of an investigation (pre-warrant) and if that investigation matures then police would use the CNA in applying for a warrant or other court order to collect evidence. It is inefficient and ineffective to require CNA through a warrant process at a preliminary stage).**
  - **Fast moving, time sensitive investigations (e.g., abductions and child abuse) where there is no time to get a warrant**

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RCMP
ROYAL CANADIAN MOUNTED POLICE

Should law enforcement have warrantless access to CNA information?

- **Obtaining warrants in the early stages of a criminal investigation may not be possible as police simply might not yet have gathered sufficient information to meet the grounds necessary to be able to apply for a warrant.**

- **Obtaining warrants for general policing duties is not possible because no criminal offence is under investigation hence obtaining a warrant is not an option.**

- **For either purpose, investigative or to perform general policing duties, it is the position of the police that obtaining a warrant for basic customer identifying information such as CNA information is not required by the law.**

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada 10

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RCMP
ROYAL CANADIAN MOUNTED POLICE

Concerns About Warrants for CNA

- **Obtaining timely CNA information with a warrant in fast-moving or time sensitive investigations such as multi-million dollar Internet frauds, sexual assaults or other serious crimes in progress is not practical.**
- **The time spent by police to prepare and the courts to process warrant applications for CNA is not an effective or efficient use of limited criminal justice resources.**
- **If a new warrant was created for police to obtain CNA from TSPs, then all the police requests that TSPs are voluntarily meeting right now would have to be processed as warrants potentially leading to additional strains on the courts.**
- **Police do not know across Canada, in all jurisdictions, how many CNA requests TSPs are answering voluntarily each year. However, RCMP does know that in 2008-09, three of Canada's estimated 400 TSPs processed 600+ CNA requests for RCMP NCECC.**

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RCMP
ROYAL CANADIAN MOUNTED POLICE

The Gap Between the Law and Voluntary Release of CNA

- **Section 8 of the Charter protects information that attracts a "reasonable expectation of privacy".**

- **The Supreme Court of Canada has affirmed in a number of cases, such as *Plant,* that a person's non-core biographical information does not attract a reasonable expectation of privacy.**

- **As of 2008, a body of case law has emerged in the lower courts expressly considering whether police can seek voluntary disclosure from an ISP of a customer's name and address only, for the purposes of a child pornography investigation, by making a request without a warrant and whether or not there is a reasonable expectation of privacy in that information.**

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RCMP
ROYAL CANADIAN MOUNTED POLICE

The Gap Between the Law and Voluntary Release of CNA

- **In January 2008, an Ontario lower court ruled in *Kwok* that police should have obtained a warrant for the release of CNA information from an ISP for a child pornography investigation.**

- **Since *Kwok*, there have been at least nine other lower court rulings in Ontario and one in Saskatchewan that found police investigating child pornography could lawfully obtain CNA information from Internet Service Providers (ISPs) without a warrant.**

s.16(2)

- **In spite of these rulings companies in the [redacted] steadfastly continue to refuse to provide CNA in child pornography cases unless police serve them with a warrant to release that information.**

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RCMP
ROYAL CANADIAN MOUNTED POLICE

Lawful Access – Operational Impact

- **The absence of Lawful Access legislation impacts every aspect of policing.**

- **Real life examples: sexual exploitation of children, organized crime and terrorism.**

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RCMP
ROYAL CANADIAN MOUNTED POLICE

CNA

Example 1

- **During an online child pornography investigation, a man told the undercover investigator that he was going to sexually assault his young daughter and "broadcast" or stream the assault live on the Internet.**

- **The Internet service provider (ISP) in question voluntarily provided the name of the Internet account holder. Local police immediately went to the scene and rescued the little girl.**

- **If the ISP had not voluntarily and immediately provided the information, the little girl probably would have been sexually assaulted live on the internet.**

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RCMP
ROYAL CANADIAN MOUNTED POLICE

CNA

Example 2

- **In 2007, there was an international case involving 88 Canadian IP addresses linked to the purchase of child pornography.**
- **The police requested the CNA information associated with the addresses;**

s.16(2)

- [redacted]
- **Police were able to investigate several of the suspects for which CNA information was provided by the service provider and several charges were laid.**

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RCMP
ROYAL CANADIAN MOUNTED POLICE

CNA

Example 3

- **In Operation Koala, a major international child pornography case that came to light in January 2008, Europol provided the RCMP with information relating to 98 Canadian e-mail accounts or IP addresses.**

s.16(2)

- **The ISPs in question were asked to provide information, and a number of ISPs provided their customers' names and addresses**
- **The investigation led to the arrest and prosecution of 9 Canadians.**
-

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RCMP
ROYAL CANADIAN MOUNTED POLICE

CNA

Example 4

s.16(2)

- [redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RCMP
ROYAL CANADIAN MOUNTED POLICE

CNA

Example 5

s.16(2)

- [redacted]
- [redacted]
- [redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RCMP
ROYAL CANADIAN MOUNTED POLICE

CNA

Example 5 continued

- **The service providers would not provide police with the customer address information they needed to pursue the investigation in a timely and efficient manner.**
- [redacted]

s.16(2)

-
-

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RCMP
ROYAL CANADIAN MOUNTED POLICE

Interception Capability

Example 1

s.16(2)

- [redacted]
- [redacted]

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada 21

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RCMP
ROYAL CANADIAN MOUNTED POLICE

Interception Capability

Example 2

s.16(2)

- [redacted]
- [redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Conclusion

- **It is essential in the prevention, investigation and prosecution of child sexual exploitation, organized crime, threats to national security, and other serious offences that:**
- **Police have legislated warrantless access to customer name and address information; and**
- **Telecommunication Service Providers are required to develop and maintain intercept capable systems.**

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Hawrylak, Maciek

From: Douglas.Pentland@bc-cb.gc.ca
Sent: October-27-11 10:14 AM
To: Kwavnick, Andrea
Cc: Gernot.Kofler@bc-cb.gc.ca; William.Bradley@bc-cb.gc.ca; Hawrylak, Maciek
Subject: RE: Friday's Mtg re: Subscriber Information Stats/Examples

Good morning Andrea. We have put together two examples. We understood from our communications folks that a similar request was made through PS communications (from a meeting about a week ago). We have thus been trying to coordinate through them. In any event, I will see where they are with this information.

One point to clarify. Half the 200 requests are made through the Bureau's Resource Centre using existing databases for only public information so no problems here. The other half are made through the Canada Anti-Fraud Centre (CAFC) and this is what we believe are how many requests for BSI the Bureau actually receives. The statement about 10 of 50 TSPs being helpful is a general statement about the experience of the CAFC as a whole (all of their functions) and not necessarily only for the Bureau's work. I don't think the CAFC makes a request if they know it will not be responded to. The partners at the CAFC are the RCMP, OPP and the Bureau.

From: Kwavnick, Andrea [mailto:Andrea.Kwavnick@ps-sp.gc.ca]
Sent: Thursday, October 27, 2011 9:39 AM
To: Pentland, Douglas: CB-BC
Cc: Kofler, Gernot: CB-BC; Bradley, William: CB-BC; Hawrylak, Maciek
Subject: RE: Friday's Mtg re: Subscriber Information Stats/Examples

Good Morning,

Have you had a chance to work on scenarios and examples of how the CB would use s. 16 and how the current situation (ie: no compulsion for TSPs to provide this information) impacts on CB investigations?

CB has indicated that they make approximately 200 requests for subscriber information per year, and that only approximately 10 out of 50 TSPs provide this information. Is there any way to determine how many of the 200 requests go unanswered?

Do you think we could get something by the end of the week?

Thanks
Andrea

From: Douglas.Pentland@bc-cb.gc.ca [mailto:Douglas.Pentland@bc-cb.gc.ca]
Sent: October 12, 2011 9:24 AM
To: Kwavnick, Andrea
Cc: Gernot.Kofler@bc-cb.gc.ca; William.Bradley@bc-cb.gc.ca; Hawrylak, Maciek
Subject: RE: Friday's Mtg re: Subscriber Information Stats/Examples

The 200 requests per year is the number we have come up with. To clarify, the 10 out of 50 TSPs that provide information is from our analyst / employee at the Canada Anti-Fraud Centre (CAFC or formerly Phonebusters). The CAFC is a joint RCMP, OPP and Bureau organization based out of North Bay. Our analyst does work for both the Bureau and CAFC. I believe that this number is more from the type of work being done for the CAFC but will verify that. As for the scenarios and examples, William will be putting this together. He will try to get something for the end of the week but it may slip till early next week as he has another urgent matter that he is working on.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

From: Kwavnick, Andrea [mailto:Andrea.Kwavnick@ps-sp.gc.ca]
Sent: Wednesday, October 12, 2011 8:34 AM
To: Pentland, Douglas: CB-BC
Cc: Kofler, Gernot: CB-BC; Bradley, William: CB-BC; Hawrylak, Maciek
Subject: Friday's Mtg re: Subscriber Information Stats/Examples

Hi Doug,

At Friday's meeting Gernot and William provided some stats from the CB - the Bureau makes approximately 200 requests/year for subscriber information and only about 10 out of 50 TSPs regularly provide the information requested.

Further to the stats, we talked about CB providing some scenarios/examples of when/how subscriber information is used in your investigations. Do you think you could provide this information by the end of the week?

Thanks
Andrea

s.14
s.15(1) - Subv
s.19(1)
s.21(1)(b)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Scott, Marcie

From: Bernard Tremblay <Bernard.Tremblay@rcmp-grc.gc.ca>
Sent: January-30-12 12:55 PM
To: Scott, Marcie
Subject: Intercepts
Attachments: RCMP Hookups 2007-2009.pdf

Hi Marci,

Hook-ups attached. If you want authorizations, we have the federal numbers from the annual report of the Min.

As for warrantless intercepts, I would guess that we do 5-15 hook-ups per year under 184.4 (I assume you are not asking about 184.1).

Bernie

>>> "Scott, Marcie" <Marcie.Scott@ps-sp.gc.ca> 2012-01-30 12:43 >>>
As discussed. Marie-Anick will follow up with you shortly.
Marcie Scott
613-949-5886

[redacted]

De : Maillé, Marie Anick [mailto:MarieAnick.Maille@ps-sp.gc.ca]
Envoyé : 19 janvier 2012 15:35
À : [redacted]
Cc : Kingsley, Michèle
Objet : RE: Coordonnées
Bonjour [redacted]
Nous vous remercions beaucoup pour votre temps aujourd'hui. Il s'agit d'une question fort complexe et ce genre de discussion nous aide tous à en comprendre davantage tous les paramètres. Tel que promis, vous trouverez dans ce

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

courriel mes coordonnées ainsi que celles de ma directrice, Michèle Kingsley. N'hésitez surtout pas à communiquer avec nous pour toute question ou tout commentaire.

Au plaisir de continuer de travailler avec vous et vos collègues [redacted] dans le futur.

s.14
s.21(1)(b)

Marie Anick

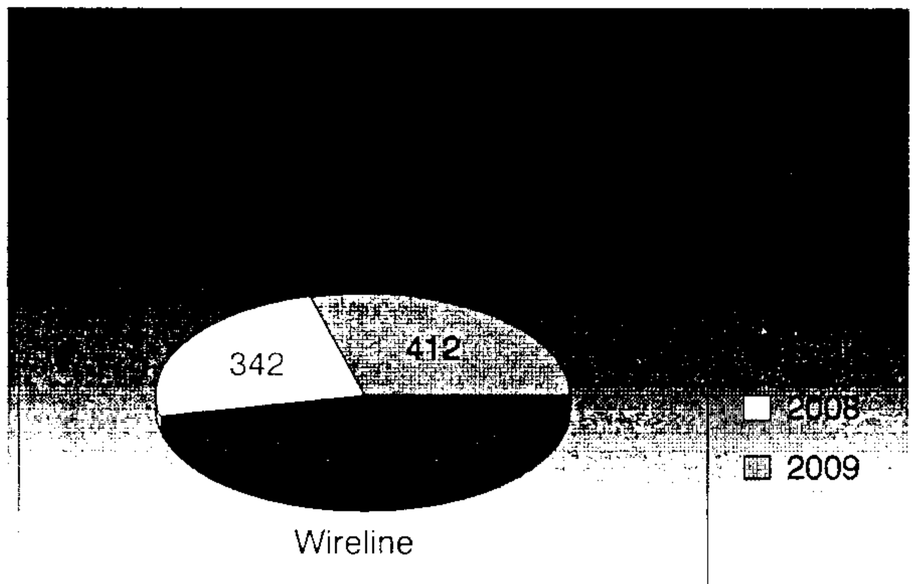
Marie Anick Maillé
Senior Policy Advisor | Conseillère principale en politiques
National Security Technology | Technologie en matière de sécurité nationale
National Security Operations Directorate | Direction générale des opérations de sécurité nationale
Public Safety Canada | Sécurité publique Canada
340 avenue Laurier Ave | Ottawa ON K1A 0P9
Telephone | Téléphone: 613.991.3240
E-mail | Courriel: marieanick.maille@ps-sp.gc.ca

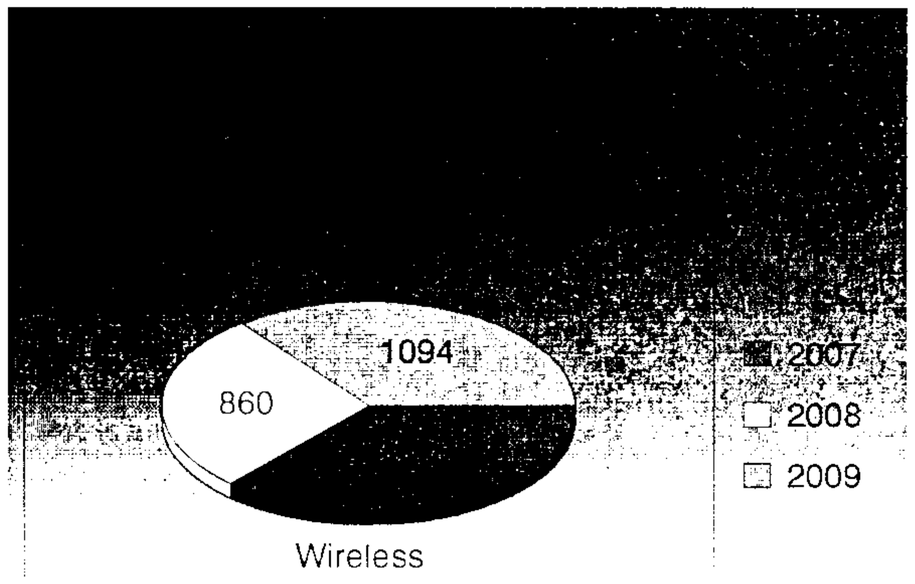
Michèle Kingsley
Director, Investigative Technologies and Telecommunications Policy | Directrice, Technologies d'enquêtes et politiques des télécommunications
National Security Operations | Opérations de la sécurité nationale
Public Safety Canada | Sécurité publique Canada
613.949.3181 / michele.kingsley@ps-sp.gc.ca

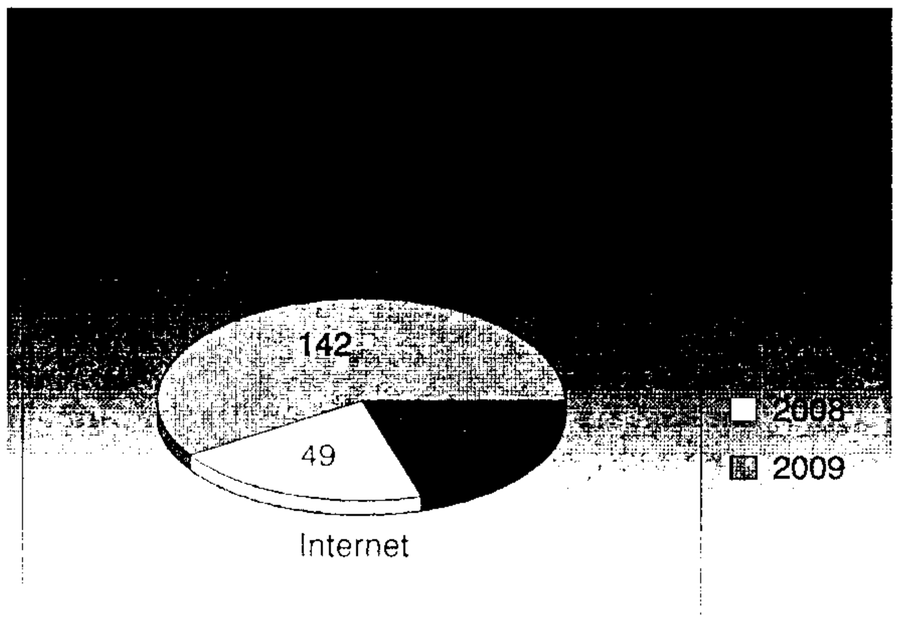
Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

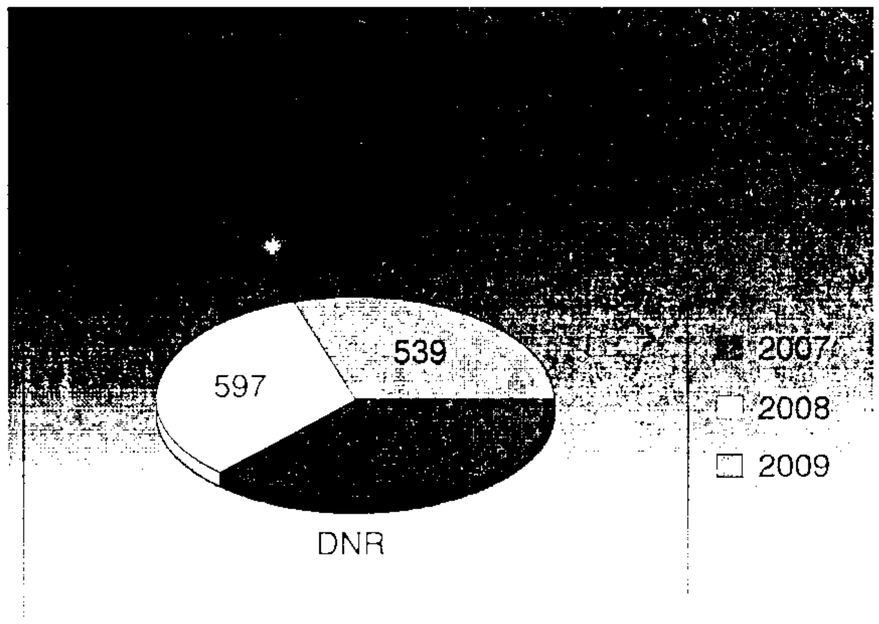
RCMP Hook-ups

Year	Wireline	Wireless	Internet	DNR	Total
2007	659	1132	49	668	2508
2008	342	860	49	597	1848
2009	412	1094	142	539	2187
3 Yr. Av.	220	1029	80	601	2181
1st half 2010			40		









Pages 108 to / à 115

are duplicates of

sont des duplicatas des

pages 144 to / à 151

Pages 116 to / à 120

are duplicates of

sont des duplicatas des

pages 139 to / à 143

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Hawrylak, Maciek

From: MacDonald, Michael
Sent: February-13-12 2:35 PM
To: Kingsley, Michèle; Kwavnick, Andrea
Cc: Maillé, Marie Anick; Hawrylak, Maciek; Scott, Marcie
Subject: FW: CACP Lawful Access Legislation examples

FYI

From: [redacted] **s.19(1)**
Sent: February-13-12 1:23 PM
To: MacDonald, Michael
Cc: Timothy M. Smith; Warren Lemcke
Subject: CACP Lawful Access Legislation examples

Michael - as requested, enclosed are the examples which we have collected. Couple of comments regarding them:

- OPP will be providing further examples momentarily. Of note is that, on their own, they make 10,000 such requests to telcos/ISP's. You can imagine the workload of police services if a warrant is required for such information. VPS estimates they would have to hire 6-8 personnel to do the paperwork for obtaining warrants.

- while it is apparent that various police services find ways to work with their telco's/ISP's, there is no consistency/obligation of a telco/ISP as you well know.

- the examples provided have not been vetted as of yet for privacy concerns. Pls keep that in mind should they be used publicly (we have to take the names of individuals out.

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

Government Relations and Strategic Communications

Canadian Association of Chiefs of Police

Begin forwarded message:

s.19(1)

From: [redacted] <[redacted]@vpd.ca>
Date: 13 February, 2012 12:05:01 PM EST

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

To: [redacted]

s.19(1) **Subject: FW: Lawful Access Legislation examples**

[redacted]

Here is a draft of the submissions presented. Can you ask PSC if they can work with this. I have not had time to put them into any kind of order.

s.19(1) [redacted]
Investigation Division
Vancouver Police Department
[redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Hawrylak, Maciek

From: Bernard Tremblay <Bernard.Tremblay@rcmp-grc.gc.ca>
Sent: February-13-12 5:52 PM
To: Kingsley, Michèle; Hawrylak, Maciek
Subject: Fw: 911 Calls in Northern Manitoba
Attachments: 911 Calls in Northern Manitoba

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Hawrylak, Maciek

From: Bernard Tremblay <Bernard.Tremblay@rcmp-grc.gc.ca>
Sent: February-13-12 4:21 PM
To: Jackie Basque
Cc: Brigitte Mineault; Helene Van Dyke; Spendlove, Jim; Mark Flynn; Stan Burke
Subject: 911 Calls in Northern Manitoba

Hi Brigitte,

Here's the 911 example.

Bernie

In the Thompson Manitoba area, 911 hang-up/incomplete calls are very frequent. When the Manitoba 911 dispatch centre notifies the RCMP of such a call, they are often only able to provide the cell phone number from which the call originated. The RCMP's first step when responding is to call that number to follow-up. If they are unable to speak to anyone to get more information, they request the name and address of the subscriber from the Telecommunications Service Provider. Very frequently, the TSP refuses to provide the RCMP with anything but GPS coordinates collected at the time the 911 call was made. Although the RCMP can then go to that area, it is often very difficult for them to locate the caller and to effectively respond to the emergency call. Some TSPs' refusal to provide the subscriber's name and address without a court order has a very direct impact on the RCMP's ability to respond to 911 calls.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Kingsley, Michèle

From: MacDonald, Michael
Sent: February-13-12 7:42 PM
To: Morris, Meribeth; Johnson, Mark
Cc: Dussault, Josée; Coburn, Stacey; Koops, Randall; Cintrat, Jean; Easson, Grant; Chang, Anna; Kingsley, Michèle; Kwavnick, Andrea; MacDonald, Michael
Subject: Fw: Document traduit - BSI examples
Attachments: Document français pour Craig.docx

As requested, attached pls find the BSI examples translated.

Mike

From: Oldham, Craig
Sent: Monday, February 13, 2012 07:31 PM
To: MacDonald, Michael
Subject: Fw: Document traduit

Here you are Mike.

S. Craig Oldham

Director General / Directeur général

Government Operations Centre / Centre des opérations du gouvernement

s.19(1) s.16(2)

613-991-7728 (T) [redacted] (C) [redacted] (S)Craig.Oldham@opscen.gc.ca

---

From: GOC-COG
Sent: Monday, February 13, 2012 07:30 PM
To: Oldham, Craig
Subject: Document traduit

Craig

Voici votre document bel et bien traduit.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted] s.16(2)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

1) En décembre 2010, des agents de la GRC du Nouveau-Brunswick ont commencé à enquêter sur des échanges pair à pair de pornographie juvénile. Ils soupçonnaient que jusqu'à 170 adresses IP étaient associées à un seul individu. Étant donné que ces adresses appartenaient à un fournisseur de services connu pour refuser de communiquer volontairement des renseignements sur ses abonnés, les policiers ont demandé à un juge de délivrer une ordonnance.

En conséquence, les renseignements de base sur l'abonné ont été fournis 15 jours plus tard. Le suspect avait alors mis fin à ses activités sur Internet. En septembre 2011, le suspect a repris ses activités en ligne. Le fournisseur a alors transmis volontairement les renseignements de base. La police a alors pu agir rapidement et arrêter le suspect chez lui en octobre 2011. Le suspect a été accusé de possession et de distribution de pornographie juvénile. La police a découvert qu'il produisait aussi des images de pornographie juvénile et a porté des accusations en conséquence. En outre, le suspect a plaidé coupable à d'autres accusations, notamment d'avoir agressé deux jeunes garçons du Nouveau-Brunswick. Si les policiers avaient pu obtenir ces renseignements dès le début de l'enquête, ils auraient pu procéder plus rapidement à l'arrestation du suspect et mettre fin aux actes de violence sexuelle commis par celui-ci.

2) [redacted]

s.16(2)

3) En 2009, des agents de la GRC en Alberta ont été informés qu'une personne avait menacé en ligne de tirer des coups de feu dans une école. Les policiers avaient en leur possession l'adresse IP utilisée par le suspect ainsi que la date et l'heure où la menace avait été proférée. Ils ont demandé au FST de leur transmettre des renseignements de base sur l'abonné. Le fournisseur de services a refusé de collaborer; il a indiqué que cette situation n'était pas une urgence, car la menace avait été proférée six jours plus tôt. Le jour suivant (un vendredi précédant une longue fin de semaine), les policiers ont demandé une ordonnance de communication afin que le FST soit contraint de transmettre les renseignements demandés. Lorsque l'ordonnance de communication a été émise, la personne-ressource du FST n'était plus au travail et les policiers ont dû attendre trois jours de plus avant

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

d'obtenir les renseignements. Une fois que le FST a eu fourni les renseignements, les policiers ont pu les utiliser afin d'obtenir un mandat supplémentaire leur permettant d'effectuer une perquisition à un domicile. Une jeune personne a été arrêtée; elle a été détenue en attendant son évaluation psychiatrique.

4) Un enfant a été enlevé en Colombie-Britannique en 2011. Une alerte Amber a été déclenchée et, heureusement, le suspect a libéré l'enfant. Toutefois, le suspect n'a pas été arrêté et l'on ne savait pas où il était. En poursuivant son enquête, la police a réussi à obtenir une adresse IP liée au suspect. La police a communiqué directement avec le FST. Ce dernier a indiqué qu'il était contraire à sa politique de fournir des renseignements sur un abonné à partir d'une adresse IP sans une ordonnance de communication. La police a informé le FST que le suspect avait déjà enlevé un enfant et que d'autres enfants pourraient être en danger. Le FST a décidé de transmettre les renseignements à la police; dans les 24 heures qui ont suivi, le suspect a été localisé et arrêté.

s.16(2)

5) [redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Hawrylak, Maciek

From: MacDonald, Michael
Sent: February-14-12 9:44 AM
To: Hawrylak, Maciek
Subject: FW: FW: Top 5 Lawful Access Examples

FYI

From: Bernard Tremblay [mailto:Bernard.Tremblay@rcmp-grc.gc.ca]
Sent: February-14-12 9:44 AM
To: MacDonald, Michael
Cc: Kwavnick, Andrea; Kingsley, Michèle
Subject: Re: FW: Top 5 Lawful Access Examples

Operation Carole is not in these 5.

Bernie

>>> "MacDonald, Michael" <Michael.MacDonald@ps-sp.gc.ca> 2012-02-14 09:40 >>>
Bernie,

Are any of these examples "Carole"?

thx

From: LeSage, Lynn
Sent: February-14-12 9:00 AM
To: MacDonald, Michael
Cc: Kingsley, Michèle
Subject: FW: Top 5 Lawful Access Examples
Importance: High

Hi Michael : pls find below some text that MO sent us last night for use by the Mins and Senator. Could you possibly take a look and let me know if you have any grave concerns with it? Thx!

From: Carmichael, Julie
Sent: Monday, February 13, 2012 6:28 PM
To: Durand, Stéphanie; Swift, Andrew; LeSage, Lynn
Cc: Patton, Michael; Johnson, Mark
Subject: FW: Top 5 Lawful Access Examples

We will need the examples below translated into French before tomorrow's announcement please and thank you.

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.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

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.

2) [redacted]

s.16(2)

3) 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.

4) 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.

5) [redacted]

s.16(2)

Julie Carmichael
Press Secretary | Attachée de presse
Office of the Minister of Public Safety | Cabinet du ministre de la Sécurité publique

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Kwavnick, Andrea

From: Kingsley, Michèle
Sent: February-24-12 6:01 PM
To: Kwavnick, Andrea; Maillé, Marie Anick; Hawrylak, Maciek; Scott, Marcie
Subject: Fw: Intercept Capability Examples

From: Bernard Tremblay [mailto:Bernard.Tremblay@rcmp-grc.gc.ca]
Sent: Friday, February 24, 2012 06:00 PM
To: Kingsley, Michèle
Cc: Brigitte Mineault <Brigitte.Mineault@rcmp-grc.gc.ca>; Helene Van Dyke <Helene.VanDyke@rcmp-grc.gc.ca>; Jackie Basque <Jacqueline.Basque@rcmp-grc.gc.ca>; Spendlove, Jim; Mark Flynn <mark.flynn@rcmp-grc.gc.ca>; Pierre Piche <Pierre.Piche@rcmp-grc.gc.ca>; Stan Burke <Stan.Burke@rcmp-grc.gc.ca>; Susan Alter <Susan.Alter@rcmp-grc.gc.ca>; Yves Desjardins <Yves.Desjardins@rcmp-grc.gc.ca>
Subject: Intercept Capability Examples

Hi Michelle,

I see you already have the terrorism example as number 15 in the Feb. 13th version of the *Utility of Basic Subscriber Information (BSI)* document. That's the second one I was going to send you.

Here's the third one:

s.16(2) [redacted]

That's all we have for now.

See you Monday morning.

Bernie

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Kwavnick, Andrea

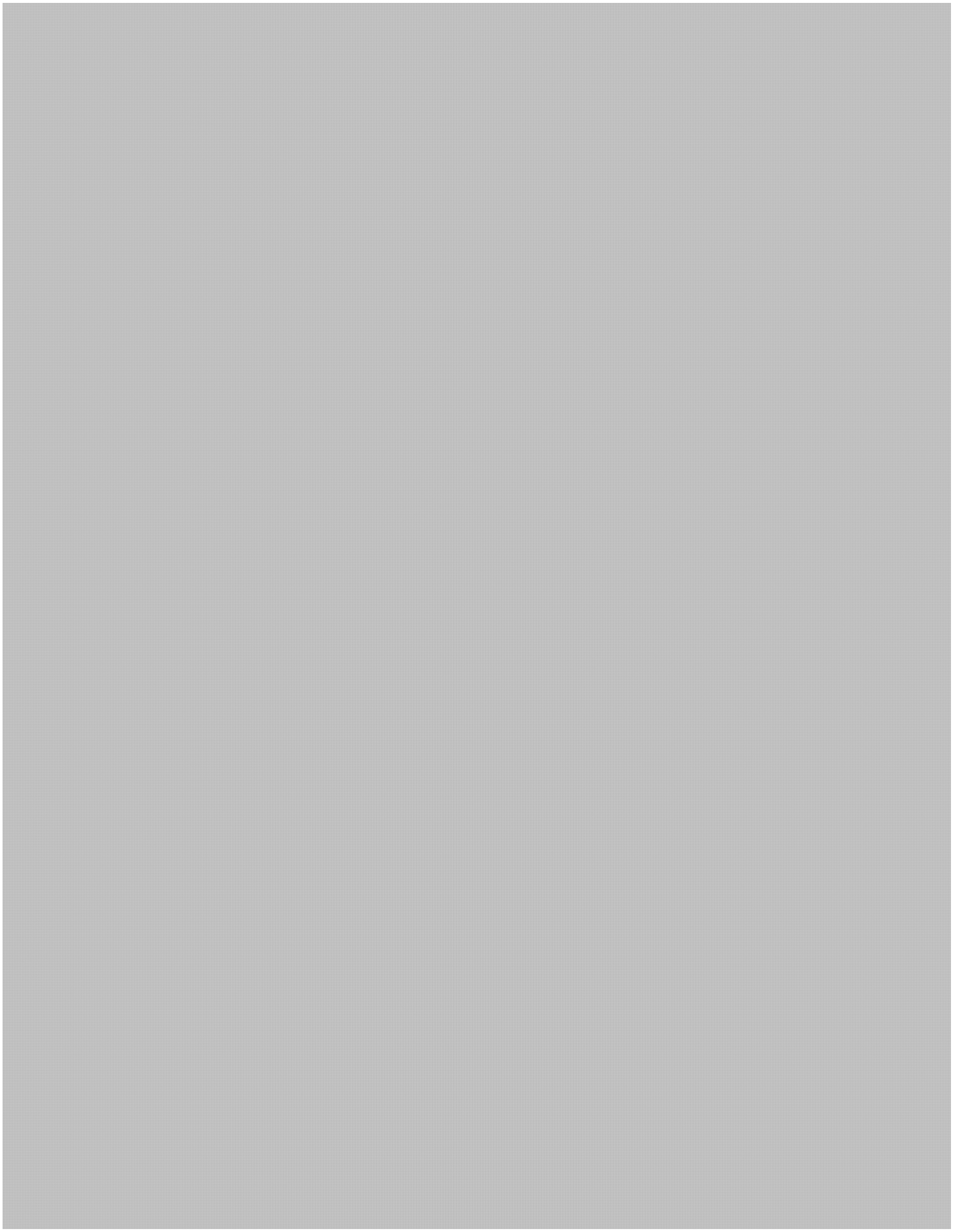
From: Kingsley, Michèle
Sent: March-13-12 11:05 AM
To: Kwavnick, Andrea; Maillé, Marie Anick; Hawrylak, Maciek; Scott, Marcie; Durand, Mathieu
Subject: Examples - Challenges experiences by the RCMP and CSIS due to a lack of interception capabilities
Attachments: Examples - Challenges experiences by the RCMP and CSIS due to a lack of interception capabilities.docx

Bonjour à tous,

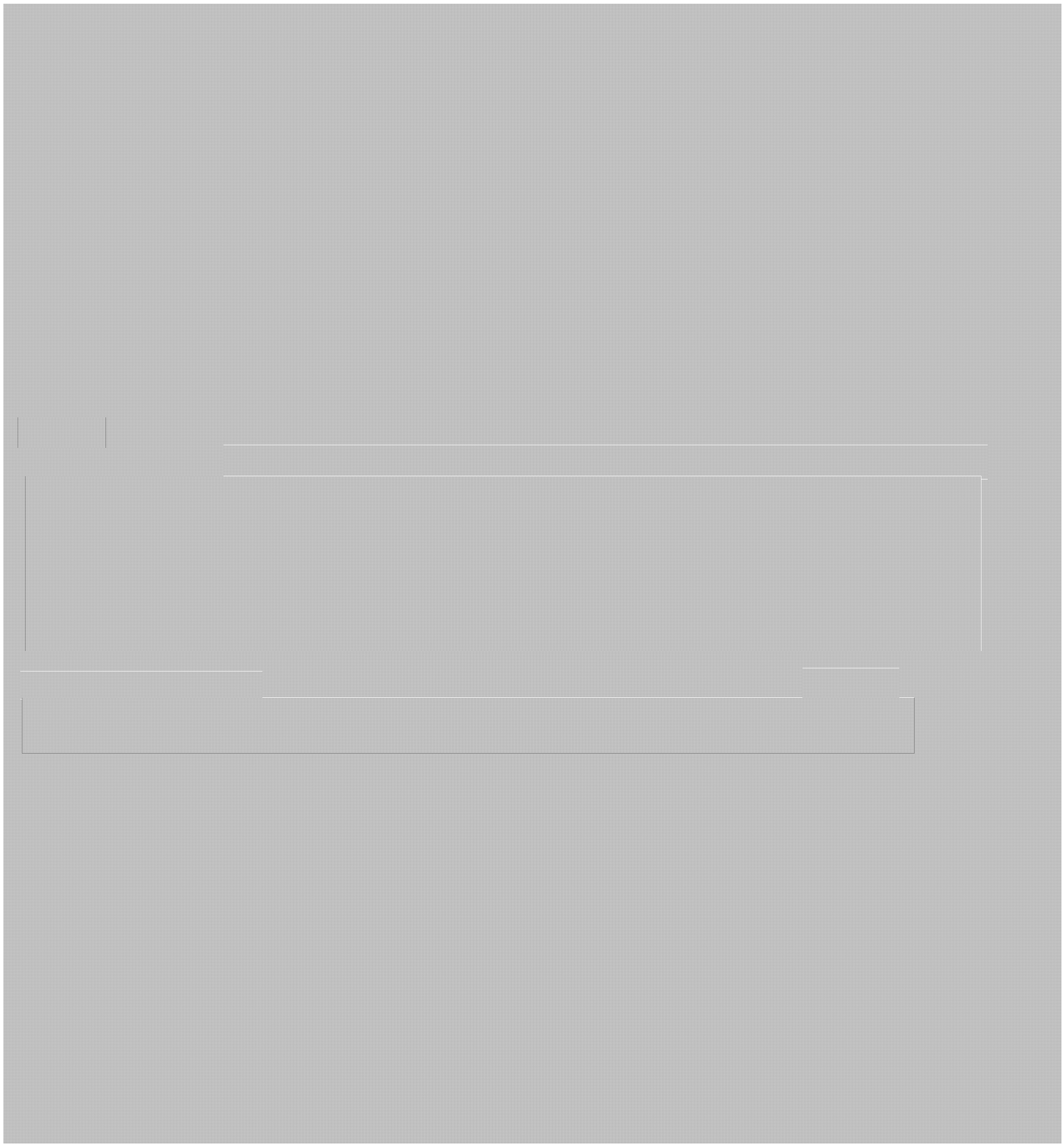
PVI, vous trouverez ci-joint un document préparé d'urgence avec la GRC et CSIS pour le bureau du ministre la semaine passée.

Michèle

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information



Pages 134 to / à 135

are duplicates of

sont des duplicatas des

pages 136 to / à 137

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Scott, Marcie

From: Kwavnick, Andrea
Sent: March-20-12 10:01 AM
To: Kingsley, Michèle; Paulson, Erika; Spendlove, Jim; [redacted]Joan Butcher (JButcher@justice.gc.ca); Burton, Meredith; Filipps, Lisa; Glazer, David; 'Greg.Scott@bc-cb.gc.ca'; Hawrylak, Maciek; Kousha, Hasti; Lauzon, Adam; Miller, Kevin; PSMediaCentre/CentredesmediasdeSP; Scott, Marcie; Willey, Chris; Wilson, Barbara
Subject: RE: Michael Geist - Halifax Police on Refusals to Provide Subscriber Data: None
Attachments: Demonstrating the Need for BasicSubscriber Information - V5 - February 2012.doc; Demonstrating the Need for BasicSubscriber Information - V5 - Fr - February 2012.doc

Hi Erika,

Attached is the examples document we prepared recently - in English and French. For media requests you may want to highlight some of the stats on the first page:

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
- In 2010, the average response time for BSI requests for the National Child Exploitation Coordination Centre in Ottawa is 13 days.

Thanks
Andrea

-----Original Message-----
From: Kingsley, Michèle
Sent: March-20-12 9:39 AM
To: Paulson, Erika; Spendlove, Jim; [redacted]Joan Butcher (JButcher@justice.gc.ca); Burton, Meredith; Filipps, Lisa; Glazer, David; 'Greg.Scott@bc-cb.gc.ca'; Hawrylak, Maciek; Kousha, Hasti; Kwavnick, Andrea; Lauzon, Adam; Miller, Kevin; PSMediaCentre/CentredesmediasdeSP; Scott, Marcie; Willey, Chris; Wilson, Barbara
Subject: RE: Michael Geist - Halifax Police on Refusals to Provide Subscriber Data: None

Thanks Erika.

Andrea will send an examples document that had been developed the week of tabling.

As background to what Mr. Geist is writing, authorities often do not have evidence of non-compliance due to the nature of the current voluntary system. To illustrate, a policy officer can ask for the information - if he/she doesn't get it, the negative response doesn't get recorded. The voluntary process is verbal. In some areas of the country, police officers don't bother asking for BSI anymore because of years of refusals from TSPs - that doesn't get recorded. In other areas, police obtain it voluntarily due to a cooperative relationship with the TSP - that doesn't get recorded either.

What's being proposed under C-30 would mandate authorities to determine - and audit - exactly what is being requested, what is being provided, and why. The findings of those audits would be reported. The Privacy Commissioner and other privacy oversight bodies could then audit those requests as well.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

If you think turning the above into a response bullet of some kind please let me know.

Merci, Michèle

Michèle Kingsley
Director, Investigative Technologies and Telecommunications Policy | Directrice, Technologies d'enquêtes et politiques des télécommunications National Security Operations | Opérations de la sécurité nationale Public Safety Canada | Sécurité publique Canada
613.949.3181 / michele.kingsley@ps-sp.gc.ca

-----Original Message-----
From: Paulson, Erika
Sent: March-19-12 12:56 PM
To: Spendlove, Jim; [redacted] Joan Butcher (JButcher@justice.gc.ca); Burton, Meredith; Filipps, Lisa; Glazer, David; 'Greg.Scott@bc-cb.gc.ca'; Hawrylak, Maciek; Kingsley, Michèle; Kousha, Hasti; Kwavnick, Andrea; Lauzon, Adam; Maillé, Marie Anick; Miller, Kevin; PSMediaCentre/CentredesmediasdeSP; Scott, Marcie; Willey, Chris; Wilson, Barbara
Subject: FYI: Michael Geist - Halifax Police on Refusals to Provide Subscriber Data: None

FYI - Geist has begun publishing results from his inquiries to local police forces RE non-compliance for voluntary disclosure of BSI by TSPs. According to his recent post, neither Montreal nor Halifax police have evidence of non-compliance. Please find the full article below.

We have a document that provides 5 examples of non-compliance that compromised an investigation, but some are old. Please find it attached. If there are more recent examples/more extensive data on non-compliance for voluntary disclosure, it would prove useful.

Relevant approved MLs are as follows:

- Basic subscriber information is often required at the early stages of investigations and is essential for pursuing investigative leads. The inability to obtain this information in a timely fashion can delay or block important investigations and undermine public safety and security.
- Police also need basic subscriber information for non-investigative purposes. For example, contacting next of kin, returning stolen property or assisting individuals in distress.
- Current federal legislation allows telecommunications service providers to release basic subscriber information to authorities without a warrant. However, they are not required to do so.
- While some service providers do release basic subscriber information to authorities upon request, others fail to provide it in a timely fashion, and others request a warrant. As a result, there is no consistency or predictability across the country when authorities request this basic information and investigations are often delayed or hampered.

Cheers,
Erika Paulson
Tel: 613-993-4415 | BB: [redacted] s.19(1)

*****

FULL ARTICLE:
http://www.michaelgeist.ca/content/view/6382/125/

Halifax Police on Refusals to Provide Subscriber Data: None

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Monday March 19, 2012

Among the government's primary justifications for its lawful access/online surveillance bill (Bill C-30) is that since Internet providers have not been required to disclose subscriber information during an investigation, their assistance is inconsistent. For example, the Public Safety backgrounder on the bill states:

Basic subscriber information is often required at the early stages of investigations or to fulfill general policing duties. This information can already be provided without a warrant under existing legislation, but only on a voluntary basis, which results in inconsistent access and delay.

RCMP data indicates that ISPs complied with nearly 95 percent of requests in 2010, suggesting that non-compliance involves a very small number of cases. I recently filed a series of access to information requests with local police forces to better identify whether they were running into problems. The answer so far is no. The request asked for "a list of all incidents since January 1, 2009 where a request to an Internet service provider for customer name, address, email address, internet protocol address, or IMEI number was refused." The Montreal Police responded that there were no records on point. The Halifax Police was very cooperative and undertook a detailed search. This is notable since Bell Aliant is sometimes identified as an ISP that seeks court orders for disclosure of subscriber information. The Halifax Police report:

A search was conducted using key words such as Bell (2022), ISP (1703), computer (540), Rogers (530), Eastlink (119), Facebook (107), Telus (96), internet (90), Aliant (66), Bell/Aliant (8), Internet Protocol (1) and Kodoo (no results). A review was undertaken and we could not find a refusal.

I'll report on other results as they come in.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Utility of Basic Subscriber Information (BSI)

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, the average response time for these requests was 13 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 provided by the RCMP

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

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

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. and police were able to investigate these individuals and in some cases charges were laid.

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.

4)

s.16(2)

5)

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

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

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.

<u>Examples of how BSI is useful to locate or identify an individual</u>

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.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

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) [redacted]

s.16(2)

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, Project Awaken, 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. [redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Examples provided by CSIS

Examples of how BSI can mitigate threats to Canadians and Canada's allies serving abroad

16) The Service received information from [redacted] At the time of receiving this information, there was no open source information linking this telephone number to a specific individual. A request to the telephone company for basic subscriber information confirmed that the number was registered to a Canadian citizen. This individual was interviewed by Canadian authorities and provided information that was used to protect our allies overseas.

17) Canadian authorities received information that a telephone number was found in the possession of an Al Qaeda associate. A request to the telephone company for basic subscriber information confirmed that the number belonged to an individual residing in Canada. The individual was interviewed by Canadian authorities, and provided information very helpful to an ongoing investigation into terrorist activities both in Canada and abroad.

Examples of how BSI can support investigations

18) The Service was investigating an individual that posed a threat to the security of Canada. When this person suddenly vacated their place of residence, authorities had difficulty re-establishing their whereabouts. After reviewing the person's telephone records (which the Service had warranted access to), basic subscriber information was requested for a number that the individual frequently called. This revealed an address that the individual often visited and permitted the investigation to resume with minimal interruption.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Utilité des renseignements de base des abonnés

L'un des problèmes du système actuel est qu'il n'y aucune uniformité ou fiabilité quant à la façon dont les télécommunicateurs répondent aux demandes de renseignements de base sur les abonnés. Par exemple :

- Il y a un télécommunicateur qui ne répond aux demandes de renseignements que le vendredi, peu importe à quel moment la demande a été soumise.
- Il y a un télécommunicateur qui n'accepte que les demandes de renseignements soumises par courriel.

Le Centre national de coordination contre l'exploitation des enfants (CNCEE) d'Ottawa a examiné un échantillon de 1 244 demandes de renseignements de base sur les abonnés parmi celles qu'il a formulées en 2010. Les télécommunicateurs ont fourni les renseignements demandés dans 902 cas (72,5 %). Toutefois, dans 62 cas (5 %), ils ont refusé de fournir les renseignements demandés sans une ordonnance de la cour et, dans 53 cas (4,3 %), ils n'ont tout simplement pas répondu aux demandes. Dans 227 cas (18,2 %), les télécommunicateurs ne disposaient pas des renseignements demandés par les autorités. Ces chiffres n'englobent pas les demandes effectuées par d'autres unités menant des enquêtes relatives à des infractions d'exploitation d'enfants par Internet au pays.

En outre, le délai moyen de réponse aux demandes est de 13 jours.

Le CNCEE d'Ottawa a signalé que sur les 482 demandes de renseignements de base sur les abonnés qu'il a faites en 2007, les télécommunicateurs ont refusé dans 19 cas (3,9 %) de fournir les renseignements sans ordonnance du tribunal et, dans 92 cas (19,1 %), ils n'ont pas donné suite à la demande. Dans 40 cas (8,3 %), les télécommunicateurs ne possédaient pas les renseignements demandés. En 2008, le CNCEE d'Ottawa a formulé 335 demandes de renseignements de base sur les abonnés. Dans six cas (1,8 %), les télécommunicateurs ont refusé de fournir les renseignements sans ordonnance du tribunal. Dans 46 cas (13,7 %), ils n'ont pas

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

répondu à la demande, et dans 30 cas (9 %), les télécommunicateurs ne possédaient pas les renseignements demandés.

Exemples fournis par la GRC

Exemples de disparité régionale concernant les télécommunicateurs qui fournissent des renseignements de base sur les abonnés

Parfois, les télécommunicateurs de certaines régions ne répondent pas aux demandes soumises par les autorités. Certains télécommunicateurs du Canada Atlantique ne fourniront des renseignements de base sur les abonnés que si les autorités ont un mandat.

1) En décembre 2010, la GRC du Nouveau-Brunswick a commencé à enquêter sur un cas d'échange de pornographie juvénile de poste à poste. Les policiers soupçonnaient que jusqu'à 170 adresses IP étaient associées à un seul individu. Puisque ces adresses IP appartenaient à un télécommunicateur reconnu pour ses refus de fournir volontairement des renseignements de base sur les abonnés en l'absence d'une ordonnance du tribunal, les policiers ont présenté une demande d'autorisation.

   Les renseignements de base sur les abonnés ont donc été fournis 15 jours plus tard et, pendant ce temps, les activités du suspect sur internet se sont arrêtées. En septembre 2011, le suspect a repris ses activités en ligne et, cette fois-là, le télécommunicateur a volontairement accepté de fournir les renseignements demandés. Cette collaboration a permis aux policiers d'agir rapidement et d'arrêter le suspect à sa résidence en octobre 2011. Le suspect a été accusé de possession et de distribution de pornographie juvénile. De plus, les policiers ont découvert qu'il produisait également du matériel de pornographie juvénile, et il a aussi été accusé pour ce crime. Le suspect a aussi plaidé coupable à des accusations qui pesaient contre lui, notamment d'avoir agressé deux jeunes garçons du Nouveau-Brunswick. Si les policiers avaient pu obtenir les renseignements demandés au début de l'enquête, ils auraient pu procéder à l'arrestation plus rapidement et ils auraient ainsi mis un terme aux agressions sexuelles commises par le suspect plus tôt.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Exemples de cas où des télécommunicateurs ont refusé de fournir des renseignements de base à la police

2) En 2007, il y a eu une affaire internationale où 88 adresses IP canadiennes ont été associées à l'achat de pornographie juvénile. Les policiers ont demandé les renseignements de base sur les abonnés associés à ces adresses. [redacted] les policiers ont donc été en mesure d'enquêter sur ces individus et, dans certains cas, des accusations ont été portées [redacted]

3) Dans le cadre de l'opération Koala portant sur une affaire de pornographie juvénile d'envergure internationale en 2008, Europol a fourni à la GRC des renseignements relatifs à 98 comptes de courriel ou adresses IP du Canada. On a demandé aux télécommunicateurs de fournir des renseignements de base relatifs à leurs clients. De nombreux télécommunicateurs ont fourni les renseignements demandés, ce qui a permis de procéder à l'arrestation de neuf Canadiens et de les traduire en justice. [redacted]

4) [redacted]

s.16(2)

5) [redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

s.16(2)

[redacted]

6) Une enquête criminelle internationale menée en 2006 comportait 78 adresses IP canadiennes associées à l'achat de pornographie juvénile. Des demandes visant à obtenir des renseignements de base sur les abonnés ont été envoyées aux télécommunicateurs pertinents. Ces derniers ont fourni des renseignements pour

[redacted]

7) En 2009, des agents de la GRC de l'Alberta ont été informés qu'une personne avait menacé en ligne de tirer des coups de feu dans une école. Les policiers avaient en leur possession l'adresse IP utilisée par le suspect ainsi que la date et l'heure où la menace avait été proférée. En outre, les policiers ont demandé au télécommunicateur de leur transmettre des renseignements pertinents sur l'abonné. Le télécommunicateur a refusé de collaborer; il a mentionné que cette situation n'était pas une urgence, car la menace avait été proférée six jours plus tôt. Le jour suivant (un vendredi précédant une longue fin de semaine), les policiers ont demandé une ordonnance de communication afin que le télécommunicateur soit contraint de transmettre les renseignements. Lorsque l'ordonnance de communication a été délivrée, la personne-ressource du télécommunicateur n'était plus au travail et les policiers ont dû attendre trois jours de plus avant d'obtenir les renseignements. Lorsque le télécommunicateur a accepté de respecter l'ordonnance de communication, les policiers ont utilisé ces renseignements afin d'obtenir un mandat supplémentaire leur permettant d'effectuer la fouille d'une demeure. Une jeune personne a été arrêtée; elle a été détenue en attendant son évaluation psychiatrique.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Exemples de l'utilité des renseignements de base sur les abonnés pour localiser ou identifier un individu

8) En 2008, le service de police de Calgary enquêtait sur des courriels de menace envoyés à une femme par un expéditeur dont l'identité était cachée. Les autorités ont donné l'adresse IP de l'auteur des courriels au télécommunicateur et lui ont demandé l'adresse municipale d'où provenaient ces derniers. Le télécommunicateur leur a donné les renseignements demandés et, en une journée, les policiers ont réussi à identifier l'individu qui envoyait les courriels de menace. Ils ont ainsi pu clore l'enquête. L'individu a été accusé de harcèlement criminel, et la victime a obtenu une ordonnance d'injonction contre lui.

9) En 2011, un enfant a été enlevé en Colombie-Britannique. Une alerte Amber a été diffusée et, heureusement, le suspect a libéré l'enfant. Toutefois, le suspect n'avait pas été appréhendé, et on ignorait où il se trouvait. En effectuant une enquête plus approfondie, les policiers ont obtenu une adresse IP associée au suspect. Ils ont donc communiqué directement avec le télécommunicateur, et on leur a répondu que, sans une ordonnance de communication, il était contraire à la politique de fournir des renseignements sur les abonnés liés à une adresse IP. Les policiers ont avisé le télécommunicateur que le suspect avait déjà enlevé un enfant et que d'autres enfants pourraient être à risque. Le télécommunicateur a alors accepté de fournir les renseignements demandés, et le suspect a été localisé et appréhendé moins de 24 heures après que les policiers ont obtenu les renseignements.

10) En 2008, le chef d'une administration municipale au Québec recevait des menaces de mort et des appels importuns. Dans ce cas, le télécommunicateur a accepté de collaborer et il a fourni les renseignements de base sur les abonnés concernés aux policiers lorsque ces derniers en ont fait la demande, ce qui leur a permis de localiser et d'arrêter le suspect. Lorsque le suspect a été appréhendé, les policiers ont saisi des armes qui se trouvaient dans sa résidence.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

11) Le service de police de Toronto a reçu au moins deux appels de citoyens l'informant qu'ils clavardaient avec des personnes menaçant de se suicider. Dans les deux cas, on ignorait où se trouvait la personne en détresse. Les policiers ont communiqué avec les hôtes des sites Web et ont réussi à obtenir les adresses IP associées aux personnes menaçant de se suicider. Ils ont ensuite pris contact avec le télécommunicateur, qui leur a fourni les renseignements de base sur les abonnés sans ordonnance du tribunal. Cela a permis aux policiers de localiser les personnes en détresse avant qu'elles ne passent de la parole aux actes.

Exemple de l'utilité des renseignements de base sur les abonnés aux premiers stades d'une enquête

12) En 2009, les policiers ont reçu un appel au sujet d'un homicide; la victime avait subi de multiples blessures causées par une arme blanche et gisait dans la rue. Les policiers ont déterminé que la personne avait été victime d'une altercation à la sortie d'un pub local. L'une des fréquentations de la victime a dit aux policiers que l'un des hommes soupçonnés d'être impliqués dans le meurtre avait appelé sur le téléphone cellulaire de la victime avant le meurtre. Les policiers ont consulté l'historique du téléphone et trouvé le numéro de téléphone cellulaire du suspect, qu'ils ont fourni au télécommunicateur. Ils ont obtenu les renseignements de base associés à ce numéro. Les policiers ont ainsi été capables d'identifier le suspect et, à partir de là, d'en identifier d'autres. Comme les policiers avaient besoin de renseignements plus détaillés que les simples renseignements de base, ils ont présenté une ordonnance de communication et ont réussi à obtenir des messages textes incriminants.

13) En 2009, le serveur d'une entreprise de 15 000 employés installée à Calgary a été piraté. Un grand nombre de données sur l'entreprise a été volé, y compris des dossiers personnels et des renseignements sur la paie. Pendant leur enquête, les policiers ont obtenu une adresse IP de l'entreprise. Ils ont donc demandé au télécommunicateur le nom et l'adresse associés à cette adresse IP. Le télécommunicateur a refusé de fournir volontairement les renseignements de base

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

aux policiers, alors ces derniers ont obtenu un mandat de perquisition, et le télécommunicateur leur a donné les renseignements cinq jours plus tard. Ces renseignements ont permis aux policiers d'obtenir un mandat de perquisition concernant une résidence au Manitoba. Grâce à celui-ci, les policiers ont saisi les ordinateurs de l'un des anciens employés de l'entreprise, mais le délai qui s'est écoulé a été néfaste pour l'entreprise, étant donné que les renseignements volés pouvaient être d'une grande utilité pour les concurrents de cette dernière.

<u>Exemples de la nécessité d'établir une capacité d'interception</u>

14) [redacted]

s.16(2)

15) La GRC a installé du matériel d'interception chez un télécommunicateur afin d'appuyer une enquête internationale liée au blanchiment d'argent et au trafic de drogues. Lors de la mise en œuvre d'une enquête internationale distincte liée au terrorisme, Project Awaken, la police a dû réaffecter le matériel d'interception utilisé dans l'enquête sur le blanchiment d'argent afin d'intercepter les communications de la principale cible terroriste. [redacted]

s.16(2)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Exemples fournis par le SCRS

Exemples de la façon dont les renseignements de base sur les abonnés peuvent atténuer les menaces pesant sur les Canadiens et les alliés du Canada en service à l'étranger

16) [redacted] Au moment où le SCRS a reçu cette information, rien ne liait l'information de source ouverte relative à ce numéro de téléphone à une personne particulière. Les renseignements de base reçus de la compagnie de téléphone ont confirmé que le numéro avait été enregistré sous le nom d'un citoyen canadien. Cette personne a été interrogée par les autorités canadiennes et elle a communiqué des renseignements qui ont permis de protéger nos alliés à l'étranger.

17) Les autorités canadiennes ont été informées qu'un numéro de téléphone avait été trouvé en possession d'une personne associée à al-Qaïda. Les renseignements de base obtenus de la compagnie de téléphone concernée ont permis de confirmer que le numéro était celui d'un résidant du Canada. La personne a été interrogée par les autorités canadiennes et a fourni de l'information très utile à une enquête qui était en cours à propos d'activités terroristes menées au Canada et à l'étranger.

Exemples de la façon dont les renseignements de base sur les abonnés peuvent appuyer les enquêtes

18) Le SCRS enquêtait sur un individu qui posait une menace à la sécurité du Canada. Lorsque cette personne a soudainement quitté sa résidence, les autorités ont eu de la difficulté à déterminer de nouveau où elle se trouvait. Après avoir examiné les relevés téléphoniques de la personne (auquel le SCRS a eu accès grâce à un

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

mandat), on a demandé à obtenir les renseignements de base de l'abonné à un numéro que l'individu appelait fréquemment. Ces renseignements ont révélé un endroit que la personne visitait souvent et ont permis la reprise de l'enquête après une période d'interruption minimale.

Pages 153 to / à 159

are not relevant

sont non pertinentes

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Kwavnick, Andrea

From: Kingsley, Michèle
Sent: March-23-12 1:38 PM
To: Kwavnick, Andrea
Subject: FW: RE: OPP Strategy Example for Bill C-30
Attachments: Fwd: RE: OPP Strategy Example for Bill C-30

From: Bernard Tremblay [mailto:Bernard.Tremblay@rcmp-grc.gc.ca]
Sent: March-23-12 10:50 AM
To: Kingsley, Michèle
Subject: Fwd: RE: OPP Strategy Example for Bill C-30

Bonjour Michèle,

Voici l'explication de Jackie.

Bernard

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Kwavnick, Andrea

From: Jackie Basque <Jacqueline.Basque@rcmp-grc.gc.ca>
Sent: March-23-12 10:26 AM
To: Bernard Tremblay
Cc: Bob Resch
Subject: Fwd: RE: OPP Strategy Example for Bill C-30
Attachments: RE: OPP Strategy Example for Bill C-30

Hi Bernie,

I just confirmed with Frank, there was 103 LER requests made as some targets had multiple locations and/or downloads. The number of requests made by OPP does not change the weight of the contents of the letter. The ISP's in this example cooperated and therefore, it is a good news story in regards to the victims being rescued in a timely manner. If the ISP's hadn't cooperated, then I could see this number having an impact on the contents of the letter.

Jackie

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Canadians are concerned about crime, particularly crime involving children.

Reported child pornography offences were up 36% in 2010 in Canada (Statistics Canada, Police-reported crime statistics in Canada, 2010).

Inspector Scott Naylor, manager of the Ontario Provincial Police child exploitation unit, said that our current system for obtaining IP addresses of suspected child pornographers isn't effective. "It's still like putting a cup under Niagara Falls. That's all we are catching".

That is why our Government has introduced the *Protecting Children from Internet Predators Act*.

We want to fix our laws while striking the right balance when it comes to protecting privacy.

Bill C-30 creates no new powers to access the content of e-mails~~, web-browsing history~~ or phone calls beyond that which already exists in Canadian law.

We will send this legislation directly to Committee for a full examination of potential amendments to achieve the best protection for our children.

Today, telecommunications service providers (TSP) may provide authorities, without a warrant, with basic subscriber information under the *Personal Information Protection and Electronic Documents Act*. The problem is that there is no consistency across the country in how service providers respond to these requests: sometimes they respond in a timely manner, but often they respond only after considerable delays, if at all.

Specifically:

Formatted: Indent: Left: 0 cm

I. According to the Royal Canadian Mounted Police's (RCMP) National Child Exploitation Coordination Centre in Ottawa, in 2010, the average response time for a basic subscriber information request was 13 days, and only 72.5% of requests were fulfilled.

II. One TSP only responds to basic subscriber information requests on Fridays, regardless of when the requests are submitted.

III. Another TSP only accepts BSI requests via email, which can be problematic in emergencies.

IV. In December 2010, New Brunswick RCMP began to investigate the distribution of child pornography. Police suspected an individual who was

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

using a TSP who had historically not shared information with police. As a result, local police applied for a court order. There was a substantial delay and by this time the case had gone cold as the suspect had stopped his activities. Due to this delay, abuse could have been prevented at an earlier date as it was later discovered that this suspect was abusing two ~~young~~ boys to create child pornography. Several months later, the suspect resumed his online activity. This time the TSP was cooperative with police requests. The suspect was charged with possession and distribution of child pornography. ~~Due to this delay, the abuse could have been prevented at an earlier date as it was discovered that this suspect was abusing two young boys to create child pornography.~~

V. 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 committing 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.

VI. 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 Internet Protocol (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.

[redacted] **s.21(1)(a)**

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Les Canadiens sont préoccupés par le crime, particulièrement lorsque cela implique des enfants.

Les infractions de pornographie juvéniles déclarées par la police ont augmentées de 36% en 2010. (Statistiques Canada, Statistiques sur les crimes déclarés par la police au Canada, 2010)

L'inspecteur Scott Naylor, gestionnaire de la Section de la pornographie juvénile à la Police provinciale de l'Ontario, affirme que notre système pour obtenir les adresses IP des pornographes juvéniles présumés est inefficace. « C'est comme mettre une tasse sous les chutes Niagara. C'est tout ce qui est pris. »

C'est pourquoi nous avons introduit la *Loi sur la protection des enfants contre les cyberprédateurs*.

Nous voulons modifier nos lois tout en établissant un juste équilibre avec la protection de la vie privée.

Le projet de loi C-30 ne créerait aucuns nouveaux pouvoirs d'accéder au contenu des courriels ou à des appels téléphoniques qui iraient au-delà des pouvoirs qui existent déjà dans la loi canadienne.

Nous enverrons ce projet de loi directement au comité pour un examen complet d'amendements potentiels afin d'atteindre la meilleure protection pour nos enfants.

En vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques*, les télécommunicateurs peuvent, sans qu'un mandat soit nécessaire, transmettre aux autorités des renseignements de base sur les abonnés. Or, le problème est qu'il n'y a aucune uniformité à l'échelle du pays dans la façon dont les télécommunicateurs répondent à ces demandes. Parfois, ils y donnent suite rapidement, mais parfois, ils y répondent qu'après un long délai ou n'y répondent pas du tout.

Ainsi :

Formatted: Indent: Left: 0 cm

I. En 2010, selon le Centre national de coordination contre l'exploitation des enfants de la Gendarmerie royale du Canada (GRC) d'Ottawa, le temps de réponse moyen à une demande de renseignements de base sur les abonnés était de 13 jours et seulement 72,5% des demandent furent exécutées.

II. Un certain télécommunicateur répond seulement le vendredi aux demandes de renseignements de base sur les abonnés, et ce, peu importe le moment où la requête est soumise.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

III. Un autre télécommunicateur accepte seulement les demandes de renseignements de base sur les abonnés soumises par courrier électronique. Il va sans dire que cela peut s'avérer problématique lors de situations d'urgence.

IV. En décembre 2010, la GRC du Nouveau-Brunswick a commencé à enquêter sur un cas de distribution de pornographie juvénile. Les policiers soupçonnaient un individu qui utilisait un télécommunicateur reconnu pour ne pas fournir l'information demandée aux policiers. Sachant cela, le policier local a appliqué pour une demande d'autorisation. En raison de ce délai, des abus envers des personnes mineures n'ont pas pu être prévenus à une date antérieure. De fait, il fut ultérieurement découvert que ce suspect abusait de deux garçons afin de réaliser de la pornographie juvénile. Cependant, le suspect a arrêté ses activités en ligne durant la période d'obtention du mandat donc l'enquête fut suspendue. Quelques mois plus tard, le suspect a repris ses activités en ligne et, cette fois, le télécommunicateur a accepté de fournir les renseignements demandés. Le suspect a été accusé de possession et de distribution de pornographie juvénile.

V. En 2007, la GRC a pris part à une enquête internationale visant des suspects qui se trouvaient au Canada et qui essayaient d'obtenir frauduleusement environ 100 millions de dollars de sociétés américaines. Au cours de l'enquête, les policiers devaient identifier les personnes commettant ces activités frauduleuses. Les suspects se déplaçaient constamment et les policiers avaient besoin de l'aide immédiate des télécommunicateurs pour déterminer où se trouvaient les réseaux. Cependant, les télécommunicateurs refusaient de fournir les renseignements de base sur les abonnés nécessaires. En raison du manque de collaboration des télécommunicateurs, il a fallu cinq jours à huit enquêteurs spécialisés travaillant à temps plein pour enfin trouver et arrêter les suspects, qui avaient alors déjà escroqué 15 millions de dollars à leurs victimes. Si les policiers avaient obtenu les renseignements dont ils avaient besoin lorsqu'ils les ont demandés, on aurait pu limiter considérablement le montant de la fraude et les ressources policières auraient pu être utilisées plus efficacement.

VI. Un enfant a été enlevé en Colombie-Britannique en 2011. Une alerte Amber a été diffusée et, heureusement, le suspect a libéré l'enfant. Toutefois, le suspect n'a pas alors été appréhendé, et on ignorait où il se trouvait. En effectuant une enquête plus approfondie, les policiers ont obtenu une adresse de protocole Internet (IP) associée au suspect. Ils ont donc communiqué directement avec le télécommunicateur, et on leur a répondu que, sans une ordonnance de communication, il était contraire à leur politique de fournir des renseignements sur les abonnés liés à une adresse IP. Les policiers ont avisé le télécommunicateur que le suspect

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

avait déjà enlevé un enfant et que d'autres enfants pourraient être à risque. Le télécommunicateur a alors accepté de fournir les renseignements demandés, et le suspect a été localisé et appréhendé moins de 24 heures après que les policiers ont obtenu les renseignements.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Kwavnick, Andrea

From: Slack, Jessica
Sent: April-12-12 4:47 PM
To: Kingsley, Michèle; 'Bruce.Wallace@ic.gc.ca'
Cc: Kwavnick, Andrea; Lisa.Foley@ic.gc.ca; Ken.Armstrong@ic.gc.ca; Michel.Cimpaye@ic.gc.ca
Subject: RE: HEADS UP: Notification: Media Call on Lawful Access

Ok great. Works for me. Thanks so much for your work on this.
Jessica

From: Kingsley, Michèle
Sent: April-12-12 4:44 PM
To: 'Bruce.Wallace@ic.gc.ca'
Cc: Kwavnick, Andrea; Slack, Jessica; Lisa.Foley@ic.gc.ca; Ken.Armstrong@ic.gc.ca
Subject: RE: HEADS UP: Notification: Media Call on Lawful Access

I'm ok with this.

Jessica – let's go ahead with this. Bruce and I agreed to leave the CBA's question as is.

Merci, m.

From: Bruce.Wallace@ic.gc.ca [mailto:Bruce.Wallace@ic.gc.ca]
Sent: April-12-12 4:42 PM
To: Kingsley, Michèle
Cc: Kwavnick, Andrea; Slack, Jessica; Lisa.Foley@ic.gc.ca; Ken.Armstrong@ic.gc.ca
Subject: RE: HEADS UP: Notification: Media Call on Lawful Access

Thanks, Michele:

How about:

There is no requirement to record the number of basic subscriber information requests made **by authorities**. While some agencies may decide to record this type of information, it is not mandatory. As such, this data is not available. **PIPEDA does not compel ISPs to respond to requests from authorities for subscriber information, it simply allows them to do so without contravening the Act.**

From: Kingsley, Michèle [mailto:Michele.Kingsley@ps-sp.gc.ca]
Sent: Thursday, April 12, 2012 4:19 PM
To: Wallace, Bruce: ECOM-DGCE
Cc: Kwavnick, Andrea; Slack, Jessica
Subject: RE: HEADS UP: Notification: Media Call on Lawful Access

Bruce,

How about this?

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

There is no requirement to record the number of basic subscriber information requests made **by authorities**. While some agencies may decide to record this type of information, it is not mandatory. As such, this data is not available. **PIPEDA does not compel ISPs to respond to requests from authorities for subscriber information, it allows them to do so.**

From: Slack, Jessica
Sent: April-12-12 2:34 PM
To: Kwavnick, Andrea
Cc: Kingsley, Michèle
Subject: RE: HEADS UP: Notification: Media Call on Lawful Access

Andrea, Michèle,

IC came back with some changes to Q1...let me know if you have any concerns.
Jessica

1. How many requests for ISP subscriber information are made by law enforcement each year?

There is no requirement to record the number of basic subscriber information requests made **by law enforcement**. While some agencies may decide to record this type of information, it is not mandatory. As such, this data is not available. **PIPEDA does not give law enforcement the power to make subscriber information requests. It merely permits ISPs to abide by such requests without the subscribers' consent. As such, "PIPEDA requests" do not exist.**

From: Kwavnick, Andrea
Sent: April-12-12 10:26 AM
To: Slack, Jessica
Cc: Kingsley, Michèle
Subject: HEADS UP: Notification: Media Call on Lawful Access

Hi Jessica,

Below please find our response to the media call. Mike MacDonald has approved the response, and it has also been reviewed by Industry Canada and the RCMP.

Let me know if you have any questions.

Thanks
Andrea

Here's my questions on Bill C-30 and PIPEDA and how they relate to privacy law enforcement requests for subscriber information.

1. How many PIPEDA requests for ISP subscriber information are made by law enforcement each year?

There is no requirement to record the number of basic subscriber information requests made under PIPEDA. While some agencies may decide to record this type of information, it is not mandatory. As such, this data is not available.

2. What proportion of these are related to serious crimes like child pornography and child exploitation?

As there is no requirement to record the number of basic subscriber information requests, we do not know the proportion of requests related to serious crimes.

3. Do any of these requests to ISPs get refused?

Yes, requests get refused. (See A4)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

4. What aspects of this voluntary system are not working well for law enforcement purposes?

Today, telecommunications service providers may choose to provide authorities, without a warrant, with basic subscriber information under the *Personal Information Protection and Electronic Documents Act*. The problem is that there is no consistency across the country in how service providers respond to these requests: sometimes they respond in a timely manner, but sometimes they respond only after considerable delays, if at all.

- Specifically:
  - according to the RCMP's National Child Exploitation Coordination Centre in Ottawa, in 2010, the average response time for a basic subscriber information request was 13 days, and only 72.5% of requests were fulfilled;
  - one telecommunications service provider only responds to basic subscriber information requests on Fridays, regardless of when the requests are submitted; and
  - another telecommunications service provider only accepts BSI requests via email, which can be problematic in emergencies.

This legislation will ensure that authorities will be able to perform their jobs more efficiently, while maintaining a level of accountability and transparency.

5. How do you reassure people that direct warrantless access to subscriber info would not contravene reasonable expectation of privacy as outlined in the Charter?

The legislation includes numerous safeguards to ensure that access to basic subscriber information respects the expectation of privacy attached to this type of information.

For example, the number of identifiers that authorities can receive upon request is limited to 6;only the customer name, address, email address, telephone number, IP address and name of the telecommunications service provider.

In fact, the Bill will provide more checks and balances than exist under the current system by:

- limiting the number of officials who can request basic subscriber information to a maximum of five designated officials per organization or 5% of the organization's workforce (whichever is greater);
- stipulating that requests can only be made in order to perform a duty or function of the designated official's agency;
- allowing non-designated police officers to request basic subscriber information only in specific emergency situations;
- putting procedures in place for mandatory record keeping of all requests;
- mandating regular internal audits and requiring that reports on the findings of these audits be provided to the responsible Minister and to the responsible external review bodies (such as the Privacy Commissioner); and
- requiring that telecommunications service providers comply with the confidentiality and security measures.

The Bill expressly reconfirms the role of review bodies to audit the basic subscriber information practices and procedures of the agency for which they are responsible – such as the Privacy Commissioner for the RCMP and Competition Bureau, and the Security Intelligence Review Committee for CSIS – at any time.

6. In order to calm fears over privacy why not limit warrantless access to serious crimes like child pornography and child exploitation?

We are committed to ensuring that criminals, sexual predators, gangs and terrorists cannot exploit technology to hide their illegal activities.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Basic subscriber information is necessary to investigate crimes that might not fall under the "serious crimes" category, but which nonetheless seriously affect the lives of Canadians. Online fraud is one such crime, where all police may have to go on is an email address. Fraud affected 1,107 Canadians and resulted in $5.9M in losses in February 2012 alone, according the Canadian Anti-Fraud Centre. Moreover, basic subscriber information can help police perform critical general policing functions which serve the community, such as notifying next-of-kin in a traffic accident or returning stolen property.

7. Are there any concrete examples of police investigations into serious crimes that have been held up or have failed because of the lack of direct access to subscriber information? (I do not need identifying details, just broad outlines of cases would be fine)

Here is one such example:

In 2007, the RCMP assisted with an international fraud 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.

8. Why not simply speed up the warrant process to allow law enforcement quicker or easier access to this info, whilst retaining judicial oversight?

Basic subscriber information is often required at the beginning of an investigation and is considered to be "pre-warrant" information. Furthermore, the basic subscriber information that is provided under Bill C-30 is much less intrusive than what can be obtained with a warrant. Policing also includes several responsibilities that do not involve the investigation of crimes, and as such would not be applicable in a warrant context. These general policing duties often involve police seeking to identify contact information to, for example, notify next-of-kin in a traffic accident or assist lost or runaway individuals.

From: Slack, Jessica
Sent: April-11-12 11:01 AM
To: Kwavnick, Andrea
Subject: RE: HEADS UP: Notification: Media Call on Lawful Access

Hi Andrea,

As promised, I've filled in the blanks where I could. I hope this makes sense.

If you could review and input where needed, that would be most appreciated.

Once we have this fleshed out, we can send to Michele for approval. Does that work?
Jessica
613-949-4288

Here's my questions on Bill C-30 and PIPEDA and how they relate to privacy law enforcement requests for subscriber information.

1. How many PIPEDA requests for ISP subscriber information are made by law enforcent each year?

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

2. What proportion of these are related to serious crimes like child pornography and child exploitation?

3. Do any of these requests to ISPs get refused?
(See A4)

4. What aspects of this voluntary system are not working well for law enforcement purposes?

One such example is that today, telecommunications service providers may provide authorities, without a warrant, with basic subscriber information under the *Personal Information Protection and Electronic Documents Act*. The problem is that there is no consistency across the country in how service providers respond to these requests: sometimes they respond in a timely manner, but often they respond only after considerable delays, if at all.

- Specifically:
  - according to the RCMP's National Child Exploitation Coordination Centre, in 2010, the average response time for a basic subscriber information request was 13 days, and only 72.5% of requests were fulfilled;
  - one telecommunications service provider only responds to basic subscriber information requests on Fridays, regardless of when the requests are submitted; and
  - another telecommunications service provider only accepts BSI requests via email, which can be problematic in emergencies.

The purpose of this legislation is to ensure that police will be able to perform their jobs more efficiently, while maintaining a required level of accountability and transparency. The Bill will bring existing lawful authorities up to date to ensure that law enforcement have an investigative tool kit that is tailored to modern technology.

5. How do you reassure people that direct warrantless access to subscriber info would not contravene reasonable expectation of privacy as outlined in the Charter?

This legislation has been modified as a consequence of consultations held with various stakeholders, including privacy commissioners and privacy advocates. These consultations led to significant changes designed to strengthen the privacy safeguards contained in the proposed Act.

The number of identifiers that authorities can receive upon request was reduced from 11 to 6, leaving only the customer name, address, email address, telephone number, IP address and name of the telecommunications service provider.

In fact, the Bill would provide more checks and balances than exist currently relating to requests for this type of information by:

- limiting those who can request basic subscriber information to designated officials (with an exception for emergencies), to a maximum of five designated officials per organization or 5% of the organization's workforce (whichever is greater);
- putting procedures in place for mandatory record keeping of all requests;
- stipulating that requests be made only to perform a duty or function of the designated official's agency;
- mandating regular internal audits and requiring that reports on the findings of these audits be provided to the responsible Minister and to the responsible external review bodies (such as the Privacy Commissioner); and
- requiring that telecommunications service providers comply with the confidentiality and security measures included in the regulations.

The Bill expressly reconfirms the role of review bodies to audit the basic subscriber information controls of

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

an agency within their jurisdiction – such as the Privacy Commissioner for the RCMP and Competition Bureau, and the Security Intelligence Review Committee for CSIS – at any time.

6. In order to calm fears over privacy why not limit warrantless access to serious crimes like child pornography and child exploitation?

We are committed to ensuring that criminals, sexual predators, gangs and terrorists cannot exploit technology to hide their illegal activities.

This proposed legislation is needed to provide law enforcement and CSIS with the modern investigative tools they need to help fight crime and national security threats.

7. Are there any concrete examples of police investigations into serious crimes that have been held up or have failed because of the lack of direct access to subscriber information? (I do not need identifying details, just broad outlines of cases would be fine)

Here is one such example:

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.

8. Why not simply speed up the warrant process to allow law enforcement quicker or easier access to this info, whilst retaining judicial oversight?

From: Kwavnick, Andrea
Sent: April-10-12 5:28 PM
To: Paulson, Erika; Hawrylak, Maciek; Kingsley, Michèle
Cc: Burton, Meredith; Willey, Chris; Slack, Jessica
Subject: Re: HEADS UP: Notification: Media Call on Lawful Access

Hi Erika-

Jessica Slack forwarded the media request earlier this afternoon and said she would draft a response and provide it to us tomorrow for review and approval? Is this no longer the case?

Thanks
Andrea

From: Paulson, Erika
Sent: Tuesday, April 10, 2012 05:22 PM
To: Kwavnick, Andrea; Hawrylak, Maciek; Kingsley, Michèle
Cc: Burton, Meredith; Willey, Chris
Subject: HEADS UP: Notification: Media Call on Lawful Access

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

HEADS UP – MO has been notified of a media call on Lawful Access (please find it below). We already have approved MLs that would cover a good number of these questions, but I expect if MO decides to address some of the detail you'll be prompted to advise. My Issues Management counterparts are the ones who would ask you for any input if it's required.

I'll try to let you know early once MO has decided on how they'd like to proceed.

Erika Paulson
Tel: 613-993-4415 | BB: [redacted] s.19(1)

From: Slack, Jessica
Sent: Tuesday, April 10, 2012 4:45 PM
To: Carmichael, Julie; Mueller, Mike; Johnson, Mark; Williams, Christpher
Cc: Swift, Andrew; Filipps, Lisa; LeSage, Lynn; Paulson, Erika; Picard, Josée
Subject: Notification: Media Call on Lawful Access

Good afternoon,

We've received the request below from the Canadian Bar Association National Magazine.

Action: consulting with policy. Proposed response to follow.
Jessica

Reporter's Name	[redacted]
Media Outlet	CBA National Magazine
Call Date	4/10/2012 5:00 PM
Telephone	[redacted]
E-mail address	
Deadline	4/12/2012 5:00 PM
Status	Consulting
Branch	NS
Subject	Lawful Access
Questions	Here's my questions on Bill C-30 and PIPEDA and how they relate to privacy law enforcement requests for subscriber information.

s.19(1)

1. How many PIPEDA requests for ISP subscriber information are made by law enforcent each year?
2. What proportion of these are related to serious crimes like child pornography and child exploitation?
3. Do any of these requests to ISPs get refused?
4. What aspects of this voluntary system are not working well for law enforcement purposes?
5. How do you reassure people that direct warrantless access to subscriber info would not contravene reasonable expectation of privacy as outlined in the Charter?
6. In order to calm fears over privacy why not limit warrantless access to serious crimes like child pornography and child exploitation?
7. Are there any concrete examples of police investigations into serious crimes that have been held up or have failed because of the lack of direct access to subscriber information? (I do not need identifying details, just broad outlines of cases would be fine)
8. Why not simply speed up the warrant process to allow law enforcement quicker or easier access to this info, whilst retaining judicial oversight?

Many thanks for your help. As I said it would be good to have an interview in the next couple of days.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Hawrylak, Maciek

From: Hawrylak, Maciek
Sent: April-16-12 4:53 PM
To: 'Douglas.Pentland@bc-cb.gc.ca'
Cc: 'Gernot.Kofler@bc-cb.gc.ca'
Subject: RE: For review - Q&A on number of BSI requests

Ok, thank you.

Maciek

From: Douglas.Pentland@bc-cb.gc.ca [mailto:Douglas.Pentland@bc-cb.gc.ca]
Sent: April-16-12 3:35 PM
To: Hawrylak, Maciek
Cc: Gernot.Kofler@bc-cb.gc.ca
Subject: RE: For review - Q&A on number of BSI requests

Maciek, we are trying to pull a more accurate number for you but will need a bit more time. The "1,000" we provided to you sometime in the past is too high, it will probably end of being a few hundred.

From: Hawrylak, Maciek [mailto:Maciek.Hawrylak@ps-sp.gc.ca]
Sent: Thursday, April 12, 2012 3:24 PM
To: Bernard Tremblay (Bernard.Tremblay@rcmp-grc.gc.ca); [redacted] Carole Smith; Pentland, Douglas: CB-BC; Kofler, Gernot: CB-BC; Foley, Lisa: ECOM-DGCE; 'matthew.shogilev@justice.gc.ca' (matthew.shogilev@justice.gc.ca); 'Karen Audcent (Karen.Audcent@justice.gc.ca)'
Cc: Scott, Marcie
Subject: For review - Q&A on number of BSI requests

Colleagues,

Further to the information below, PS has developed a short Q&A answering the question of how many BSI requests are made annually. I would be grateful if you could review the attachment in general and for statistical accuracy regarding your respective organization's BSI figures, by **Monday 16 April**.

Our intent is not to release this information right away, but to have it used at a future date by the minister in a public setting. As such, it will be used publicly at some point.

Thanks,
Maciek

-----Original Message-----
From: Kingsley, Michèle
Sent: March-20-12 10:11 AM
To: Bernard Tremblay
Cc: MacDonald, Michael; Kwavnick, Andrea; Scott, Marcie; Hawrylak, Maciek; Durand, Mathieu; Kousha, Hasti; Audcent, Karen; [redacted]
Subject: FW: Michael Geist - Halifax Police on Refusals to Provide Subscriber Data: None

Bernard,

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Voir l'échange ci-dessous, qui commence avec un rapport de Michael Geist selon quoi certaines forces policières n'ont pas de documentation démontrant le refus de renseignements de bases sur les abonnés. Pas surprenant, puisqu'on ne documente pas les demandes verbales et les refus verbaux...

[redacted]

[redacted] the same would be needed from CSIS.

How are we coming along with developing more interception challenge examples? Any more BSI examples?

Merci, Michèle

-----Original Message-----
From: Kingsley, Michèle
Sent: March-20-12 9:39 AM
To: Paulson, Erika; Spendlove, Jim; [redacted] Joan Butcher (JButcher@justice.gc.ca); Burton, Meredith; Filipps, Lisa; Glazer, David; 'Greg.Scott@bc-cb.gc.ca'; Hawrylak, Maciek; Kousha, Hasti; Kwavnick, Andrea; Lauzon, Adam; Miller, Kevin; PSMediaCentre/CentredesmediasdeSP; Scott, Marcie; Willey, Chris; Wilson, Barbara
Subject: RE: Michael Geist - Halifax Police on Refusals to Provide Subscriber Data: None

Thanks Erika.

Andrea will send an examples document that had been developed the week of tabling.

As background to what Mr. Geist is writing, authorities often do not have evidence of non-compliance due to the nature of the current voluntary system. To illustrate, a policy officer can ask for the information - if he/she doesn't get it, the negative response doesn't get recorded. The voluntary process is verbal. In some areas of the country, police officers don't bother asking for BSI anymore because of years of refusals from TSPs - that doesn't get recorded. In other areas, police obtain it voluntarily due to a cooperative relationship with the TSP - that doesn't get recorded either.

What's being proposed under C-30 would mandate authorities to determine - and audit - exactly what is being requested, what is being provided, and why. The findings of those audits would be reported. The Privacy Commissioner and other privacy oversight bodies could then audit those requests as well.

If you think turning the above into a response bullet of some kind please let me know.

Merci, Michèle

Michèle Kingsley
Director, Investigative Technologies and Telecommunications Policy | Directrice, Technologies d'enquêtes et politiques des télécommunications National Security Operations | Opérations de la sécurité nationale Public Safety Canada | Sécurité publique Canada
613.949.3181 / michele.kingsley@ps-sp.gc.ca

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

-----Original Message-----
From: Paulson, Erika
Sent: March-19-12 12:56 PM
To: Spendlove, Jim; [redacted]; Joan Butcher (JButcher@justice.gc.ca); Burton, Meredith; Filipps, Lisa; Glazer, David; 'Greg.Scott@bc-cb.gc.ca'; Hawrylak, Maciek; Kingsley, Michèle; Kousha, Hasti; Kwavnick, Andrea; Lauzon, Adam; Maillé, Marie Anick; Miller, Kevin; PSMediaCentre/CentredesmediasdeSP; Scott, Marcie; Willey, Chris; Wilson, Barbara
Subject: FYI: Michael Geist - Halifax Police on Refusals to Provide Subscriber Data: None

FYI - Geist has begun publishing results from his inquiries to local police forces RE non-compliance for voluntary disclosure of BSI by TSPs. According to his recent post, neither Montreal nor Halifax police have evidence of non-compliance. Please find the full article below.

We have a document that provides 5 examples of non-compliance that compromised an investigation, but some are old. Please find it attached. If there are more recent examples/more extensive data on non-compliance for voluntary disclosure, it would prove useful.

Relevant approved MLs are as follows:

- Basic subscriber information is often required at the early stages of investigations and is essential for pursuing investigative leads. The inability to obtain this information in a timely fashion can delay or block important investigations and undermine public safety and security.
- Police also need basic subscriber information for non-investigative purposes. For example, contacting next of kin, returning stolen property or assisting individuals in distress.
- Current federal legislation allows telecommunications service providers to release basic subscriber information to authorities without a warrant. However, they are not required to do so.
- While some service providers do release basic subscriber information to authorities upon request, others fail to provide it in a timely fashion, and others request a warrant. As a result, there is no consistency or predictability across the country when authorities request this basic information and investigations are often delayed or hampered.

Cheers,
Erika Paulson
Tel: 613-993-4415 | BB: [redacted] s.19(1)

*****

FULL ARTICLE:
http://www.michaelgeist.ca/content/view/6382/125/

Halifax Police on Refusals to Provide Subscriber Data: None

Monday March 19, 2012

Among the government's primary justifications for its lawful access/online surveillance bill (Bill C-30) is that since Internet providers have not been required to disclose subscriber information during an investigation, their assistance is inconsistent. For example, the Public Safety backgrounder on the bill states:

Basic subscriber information is often required at the early stages of investigations or to fulfill general policing duties. This information can already be provided without a warrant under existing legislation, but only on a voluntary basis, which results in inconsistent access and delay.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

RCMP data indicates that ISPs complied with nearly 95 percent of requests in 2010, suggesting that non-compliance involves a very small number of cases. I recently filed a series of access to information requests with local police forces to better identify whether they were running into problems. The answer so far is no. The request asked for "a list of all incidents since January 1, 2009 where a request to an Internet service provider for customer name, address, email address, internet protocol address, or IMEI number was refused." The Montreal Police responded that there were no records on point. The Halifax Police was very cooperative and undertook a detailed search. This is notable since Bell Aliant is sometimes identified as an ISP that seeks court orders for disclosure of subscriber information. The Halifax Police report:

A search was conducted using key words such as Bell (2022), ISP (1703), computer (540), Rogers (530), Eastlink (119), Facebook (107), Telus (96), internet (90), Aliant (66), Bell/Aliant (8), Internet Protocol (1) and Kodoo (no results). A review was undertaken and we could not find a refusal.

I'll report on other results as they come in.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Kwavnick, Andrea

From: Slack, Jessica
Sent: April-17-12 10:53 AM
To: Kwavnick, Andrea; 'Bernard.Tremblay@rcmp-grc.gc.ca'
Cc: 'Jacqueline.Basque@rcmp-grc.gc.ca'; 'William.Beiersdorfer@rcmp-grc.gc.ca'
Subject: RE: C-30 / PIPEDA questions

Andrea,

The reporter was referred to the RCMP media relations unit so if he is still looking for clarification, he will follow-up with them. I gave media relations at RCMP a heads-up as well...

Thanks!
Jessica

-----Original Message-----
From: Kwavnick, Andrea
Sent: April-17-12 10:45 AM
To: 'Bernard.Tremblay@rcmp-grc.gc.ca'; Slack, Jessica
Cc: 'Jacqueline.Basque@rcmp-grc.gc.ca'; 'William.Beiersdorfer@rcmp-grc.gc.ca'
Subject: Re: C-30 / PIPEDA questions

Hi Jessica,

Please see explanation below from the RCMP.

Jessica/Bernie - please note that I'm not in the office today. As the requestor is asking questions about an RCMP document, I think PS Comms should coordinate response with RCMP.

Thanks
Andrea

----- Original Message -----
From: Bernard Tremblay [mailto:Bernard.Tremblay@rcmp-grc.gc.ca]
Sent: Tuesday, April 17, 2012 08:45 AM
To: Kwavnick, Andrea
Cc: Jackie Basque <Jacqueline.Basque@rcmp-grc.gc.ca>; William Beiersdorfer <William.Beiersdorfer@rcmp-grc.gc.ca>
Subject: Re: C-30 / PIPEDA questions

Hi Andrea,

Form 6306 is an RCMP form we developed to try to obtain numbers on subscriber info requests.

The LER is a subscriber info request form that is used only in child exploitation investigations. The National Child Exploitation Coordination Centre in Ottawa has been keeping track of these.

Can you forward to Jessica please.

Thanks.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Bernie
-----Original Message-----
From: "Kwavnick, Andrea" <Andrea.Kwavnick@ps-sp.gc.ca>
To: Basque, Jackie <Jacqueline.Basque@rcmp-grc.gc.ca>
To: Tremblay, Bernard <Bernard.Tremblay@rcmp-grc.gc.ca>

Sent: 04/16/2012 16:44:21
Subject: FW: C-30 / PIPEDA questions

Hi Bernie/Jackie,

Please see the email below. I told PS Comms to have the requestor seek clarification from the RCMP as the document in question is an RCMP document.

As a reminder, it was in response to this requestor that you provided input on some Q&As last week.

Thanks
Andrea

From: Slack, Jessica On Behalf Of PS Media Relations / Relations médias SP
Sent: April-16-12 10:34 AM
To: Kwavnick, Andrea
Subject: FW: C-30 / PIPEDA questions

Hi Andrea,
We had the follow-up below from the CBA...as this is RCMP's chart, we are thinking of recommending the reporter go there for clarification...
Do you agree?
Jessica

From: [redacted] s.19(1)
Sent: April-16-12 10:22 AM
To: PS Media Relations / Relations médias SP
Subject: Re: C-30 / PIPEDA questions

Hi Jessica,
Many thanks for this.

Just want to pick up on one point - Question 4, the % of requests fulfilled. I attach a document from RCMP showing 2010 figures relating to 'Form 6306', which has a 93% success rate in CNA requests. Would you be able to explain what Form 6306 is, and the difference between that and the Law Enforcement requests?

Many thanks
[redacted] s.19(1)

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Hawrylak, Maciek

From: Hawrylak, Maciek
Sent: April-18-12 3:23 PM
To: [redacted]
Subject: RE: For review - Q&A on number of BSI requests

I know you mentioned the numbers, but do you have any other comments on the language of the answer to the question?

FYI, you'll see from the notes at the bottom that ITAC stated that it handled 1,130,000 BSI requests annually from 2006-2008.

Maciek

From: [redacted]
Sent: April-18-12 3:21 PM
To: Hawrylak, Maciek
Subject: RE: For review - Q&A on number of BSI requests

Maciek,

I have already pointed out the point about [redacted] numbers, but it is interesting . . yesterday [redacted] with our DG and ADM met with Rogers in [redacted] and Rogers indicated at this meeting [redacted] s.21(1)(b)

It would be interesting to get Bell's figures as well.

[redacted]

>>> "Hawrylak, Maciek" <Maciek.Hawrylak@ps-sp.gc.ca> 4/18/2012 2:27 pm >>>
Just as a reminder, I have not received feedback from most parties on this request. Please provide your feedback soonest.

Many thanks,
Maciek

From: Hawrylak, Maciek
Sent: April-12-12 3:24 PM
To: Bernard Tremblay (Bernard.Tremblay@rcmp-grc.gc.ca); [redacted] Carole Smith; Douglas.Pentland@bc-cb.gc.ca; Gernot.Kofler@bc-cb.gc.ca; 'Lisa.Foley@ic.gc.ca' (Lisa.Foley@ic.gc.ca); 'matthew.shogilev@justice.gc.ca' (matthew.shogilev@justice.gc.ca); 'Karen Audcent (Karen.Audcent@justice.gc.ca)'
Cc: Scott, Marcie
Subject: For review - Q&A on number of BSI requests

Colleagues,

Further to the information below, PS has developed a short Q&A answering the question of how many BSI requests are made annually. I would be grateful if you could review the attachment in general and for statistical accuracy regarding your respective organization's BSI figures, by **Monday 16 April**.

Our intent is not to release this information right away, but to have it used at a future date by the minister in a public setting. As such, it will be used publicly at some point.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

s.15(1)(d)(ii)
s.21(1)(b)

Thanks,
Maciek

-----Original Message-----
From: Kingsley, Michèle
Sent: March-20-12 10:11 AM
To: Bernard Tremblay
Cc: MacDonald, Michael; Kwavnick, Andrea; Scott, Marcie; Hawrylak, Maciek; Durand, Mathieu; Kousha, Hasti; Audcent, Karen; [redacted]
Subject: FW: Michael Geist - Halifax Police on Refusals to Provide Subscriber Data: None

Bernard,

Voir l'échange ci-dessous, qui commence avec un rapport de Michael Geist selon quoi certaines forces policières n'ont pas de documentation démontrant le refus de renseignements de bases sur les abonnés. Pas surprenant, puisqu'on ne documente pas les demandes verbales et les refus verbaux...

[redacted]

[redacted] the same would be needed from CSIS.

How are we coming along with developing more interception challenge examples? Any more BSI examples?

Merci, Michèle

-----Original Message-----
From: Kingsley, Michèle
Sent: March-20-12 9:39 AM
To: Paulson, Erika; Spendlove, Jim; [redacted] Joan Butcher (JButcher@justice.gc.ca); Burton, Meredith; Filipps, Lisa; Glazer, David; 'Greg.Scott@bc-cb.gc.ca'; Hawrylak, Maciek; Kousha, Hasti; Kwavnick, Andrea; Lauzon, Adam; Miller, Kevin; PSMediaCentre/CentredesmediasdeSP; Scott, Marcie; Willey, Chris; Wilson, Barbara
Subject: RE: Michael Geist - Halifax Police on Refusals to Provide Subscriber Data: None

Thanks Erika.

Andrea will send an examples document that had been developed the week of tabling.

As background to what Mr. Geist is writing, authorities often do not have evidence of non-compliance due to the nature of the current voluntary system. To illustrate, a policy officer can ask for the information - if he/she doesn't get it, the negative response doesn't get recorded. The voluntary process is verbal. In some areas of the country, police officers don't bother asking for BSI anymore because of years of refusals from TSPs - that doesn't get recorded. In other areas, police obtain it voluntarily due to a cooperative relationship with the TSP - that doesn't get recorded either.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

What's being proposed under C-30 would mandate authorities to determine - and audit - exactly what is being requested, what is being provided, and why. The findings of those audits would be reported. The Privacy Commissioner and other privacy oversight bodies could then audit those requests as well.

If you think turning the above into a response bullet of some kind please let me know.

Merci, Michèle

Michèle Kingsley
Director, Investigative Technologies and Telecommunications Policy | Directrice, Technologies d'enquêtes et politiques des télécommunications National Security Operations | Opérations de la sécurité nationale Public Safety Canada | Sécurité publique Canada
613.949.3181 / michele.kingsley@ps-sp.gc.ca

-----Original Message-----
From: Paulson, Erika
Sent: March-19-12 12:56 PM
To: Spendlove, Jim; [redacted] Joan Butcher (JButcher@justice.gc.ca); Burton, Meredith; Filipps, Lisa; Glazer, David; 'Greg.Scott@bc-cb.gc.ca'; Hawrylak, Maciek; Kingsley, Michèle; Kousha, Hasti; Kwavnick, Andrea; Lauzon, Adam; Maillé, Marie Anick; Miller, Kevin; PSMediaCentre/CentredesmediasdeSP; Scott, Marcie; Willey, Chris; Wilson, Barbara
Subject: FYI: Michael Geist - Halifax Police on Refusals to Provide Subscriber Data: None

FYI - Geist has begun publishing results from his inquiries to local police forces RE non-compliance for voluntary disclosure of BSI by TSPs. According to his recent post, neither Montreal nor Halifax police have evidence of non-compliance. Please find the full article below.

We have a document that provides 5 examples of non-compliance that compromised an investigation, but some are old. Please find it attached. If there are more recent examples/more extensive data on non-compliance for voluntary disclosure, it would prove useful.

Relevant approved MLs are as follows:

- Basic subscriber information is often required at the early stages of investigations and is essential for pursuing investigative leads. The inability to obtain this information in a timely fashion can delay or block important investigations and undermine public safety and security.
- Police also need basic subscriber information for non-investigative purposes. For example, contacting next of kin, returning stolen property or assisting individuals in distress.
- Current federal legislation allows telecommunications service providers to release basic subscriber information to authorities without a warrant. However, they are not required to do so.
- While some service providers do release basic subscriber information to authorities upon request, others fail to provide it in a timely fashion, and others request a warrant. As a result, there is no consistency or predictability across the country when authorities request this basic information and investigations are often delayed or hampered.

Cheers,
Erika Paulson
Tel: 613-993-4415 | BB: [redacted] s.19(1)

*****

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

FULL ARTICLE:
http://www.michaelgeist.ca/content/view/6382/125/

Halifax Police on Refusals to Provide Subscriber Data: None

Monday March 19, 2012

Among the government's primary justifications for its lawful access/online surveillance bill (Bill C-30) is that since Internet providers have not been required to disclose subscriber information during an investigation, their assistance is inconsistent. For example, the Public Safety backgrounder on the bill states:

Basic subscriber information is often required at the early stages of investigations or to fulfill general policing duties. This information can already be provided without a warrant under existing legislation, but only on a voluntary basis, which results in inconsistent access and delay.

RCMP data indicates that ISPs complied with nearly 95 percent of requests in 2010, suggesting that non-compliance involves a very small number of cases. I recently filed a series of access to information requests with local police forces to better identify whether they were running into problems. The answer so far is no. The request asked for "a list of all incidents since January 1, 2009 where a request to an Internet service provider for customer name, address, email address, internet protocol address, or IMEI number was refused." The Montreal Police responded that there were no records on point. The Halifax Police was very cooperative and undertook a detailed search. This is notable since Bell Aliant is sometimes identified as an ISP that seeks court orders for disclosure of subscriber information. The Halifax Police report:

A search was conducted using key words such as Bell (2022), ISP (1703), computer (540), Rogers (530), Eastlink (119), Facebook (107), Telus (96), internet (90), Aliant (66), Bell/Aliant (8), Internet Protocol (1) and Kodoo (no results). A review was undertaken and we could not find a refusal.

I'll report on other results as they come in.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Myth: Police have not proven that some telecommunications service providers refuse to voluntarily disclose basic subscriber information in a timely manner, thereby delaying investigations.

Fact: The police have provided many examples where investigations have been delayed as a result of telecommunications service providers refusing to voluntarily provide basic subscriber information, some of which are provided below. Providing exact numbers of the rates of refusal is difficult as today there is no requirement for authorities to maintain records of requests for basic subscriber information.

Often, the police know, based on years of automatic refusals, that a telecommunications service provider will refuse to provide basic subscriber information, and therefore decide not to request the information at all. The police do not necessarily document refusals that have become the norm in certain parts of the country.

Here are some of the facts we do know:

- The current voluntary system has no uniformity or reliability as to how or whether service providers respond to these requests. As a result, investigations are often hampered and public safety undermined.

- There is one telecommunications service provider that only responds to requests for basic subscriber information on Fridays, regardless of when the requests are submitted. Another provider only accepts requests for basic subscriber information via email, which is problematic in emergency situations.

- The RCMP's National Child Exploitation Coordination Centre in Ottawa examined 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.[1]

- In 2010, the average response time to basic subscriber information requests from the National Child Exploitation Coordination Centre in Ottawa was 13 days. This response time of almost two weeks represents countless situations in which the exploitation of children continued because telecommunications service providers did not provide basic subscriber information in a timely manner.

- Specific cases where telecommunications service providers did not voluntarily provide police with basic subscriber information include:

    - In December 2010, New Brunswick RCMP began to investigate a case of peer-to-peer sharing of child pornography. The police investigation was impeded due to the requirement to provide the telecommunications service provider with a court order, by which time the suspect's Internet activity had stopped. When the suspect resumed his online activity in

[1] In 227 cases (18.2%) the TSPs did not have the particular information that authorities requested.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

September 2011, the service provider voluntarily provided the basic subscriber information and it was discovered he had been distributing and producing child pornography. The suspect was arrested and charged with these crimes.

- In 2008, a major international child pornography case dubbed Operation Koala provided the RCMP with information relating to 98 Canadian e-mail accounts or IP addresses. Many telecommunications service providers voluntarily provided basic subscriber information, leading to the arrest and prosecution of nine Canadians. However, the identity of 25 IP addresses or e-mail accounts could not be established due to the lack of cooperation of some service providers.
- In 2007, the RCMP assisted with an international fraud investigation. Police needed the immediate support of telecommunications service providers to determine the location of unsecured wireless computer networks, but due to lack of cooperation, it took eight full-time technical investigators five days to finally locate and arrest the suspects. Had police been provided the information when it was requested, the suspects could have been apprehended sooner and the extent of the $15 million fraud would have been reduced considerably.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Hawrylak, Maciek

From: Hawrylak, Maciek
Sent: May-11-12 12:19 PM
To: 'Douglas.Pentland@bc-cb.gc.ca'
Cc: Gernot.Kofler@bc-cb.gc.ca
Subject: RE: For review - Q&A on number of BSI requests

Thanks. I think I'm done bothering you for the moment!

Maciek

From: Douglas.Pentland@bc-cb.gc.ca [mailto:Douglas.Pentland@bc-cb.gc.ca]
Sent: May-11-12 12:19 PM
To: Hawrylak, Maciek
Cc: Gernot.Kofler@bc-cb.gc.ca
Subject: RE: For review - Q&A on number of BSI requests

[redacted]

From: Hawrylak, Maciek [mailto:Maciek.Hawrylak@ps-sp.gc.ca]
Sent: Friday, May 11, 2012 11:26 AM
To: Pentland, Douglas: CB-BC
Cc: Kofler, Gernot: CB-BC
Subject: RE: For review - Q&A on number of BSI requests

Ok, thanks. [redacted]

Maciek

From: Douglas.Pentland@bc-cb.gc.ca [mailto:Douglas.Pentland@bc-cb.gc.ca]
Sent: May-11-12 11:16 AM
To: Hawrylak, Maciek
Cc: Gernot.Kofler@bc-cb.gc.ca
Subject: RE: For review - Q&A on number of BSI requests

[redacted]

From: Hawrylak, Maciek [mailto:Maciek.Hawrylak@ps-sp.gc.ca]
Sent: Friday, May 11, 2012 11:00 AM
To: Pentland, Douglas: CB-BC
Cc: Kofler, Gernot: CB-BC
Subject: RE: For review - Q&A on number of BSI requests

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

[redacted]

Thanks,
Maciek

From: Douglas.Pentland@bc-cb.gc.ca [mailto:Douglas.Pentland@bc-cb.gc.ca]
Sent: May-11-12 10:57 AM
To: Hawrylak, Maciek
Cc: Gernot.Kofler@bc-cb.gc.ca
Subject: RE: For review - Q&A on number of BSI requests

[redacted]

From: Hawrylak, Maciek [mailto:Maciek.Hawrylak@ps-sp.gc.ca]
Sent: Thursday, May 10, 2012 3:35 PM
To: Pentland, Douglas: CB-BC
Cc: Kofler, Gernot: CB-BC
Subject: RE: For review - Q&A on number of BSI requests

Doug,

Thanks for this. [redacted]

Thanks,
Maciek

From: Douglas.Pentland@bc-cb.gc.ca [mailto:Douglas.Pentland@bc-cb.gc.ca]
Sent: May-04-12 2:36 PM
To: Hawrylak, Maciek
Cc: Gernot.Kofler@bc-cb.gc.ca
Subject: RE: For review - Q&A on number of BSI requests

Maciek, sorry for the delay in responding to this request. Here is our response:

[redacted]

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

From: Hawrylak, Maciek [mailto:Maciek.Hawrylak@ps-sp.gc.ca]
Sent: Monday, April 30, 2012 2:49 PM
To: Pentland, Douglas: CB-BC
Cc: Kofler, Gernot: CB-BC
Subject: Re: For review - Q&A on number of BSI requests

[redacted]

Thanks for doing this so diligently!

Maciek

From: Douglas.Pentland@bc-cb.gc.ca [mailto:Douglas.Pentland@bc-cb.gc.ca]
Sent: Monday, April 30, 2012 02:14 PM
To: Hawrylak, Maciek
Cc: Gernot.Kofler@bc-cb.gc.ca <Gernot.Kofler@bc-cb.gc.ca>
Subject: RE: For review - Q&A on number of BSI requests

Maciek, one further question. [redacted]

Thanks.

From: Hawrylak, Maciek [mailto:Maciek.Hawrylak@ps-sp.gc.ca]
Sent: Tuesday, April 24, 2012 1:33 PM
To: Pentland, Douglas: CB-BC
Cc: Kofler, Gernot: CB-BC
Subject: Re: For review - Q&A on number of BSI requests

Doug,

[redacted]

Maciek

From: Douglas.Pentland@bc-cb.gc.ca [mailto:Douglas.Pentland@bc-cb.gc.ca]
Sent: Tuesday, April 24, 2012 11:58 AM
To: Hawrylak, Maciek
Cc: Gernot.Kofler@bc-cb.gc.ca <Gernot.Kofler@bc-cb.gc.ca>
Subject: RE: For review - Q&A on number of BSI requests

Maciek, [redacted]

Thanks.

From: Hawrylak, Maciek [mailto:Maciek.Hawrylak@ps-sp.gc.ca]
Sent: Thursday, April 12, 2012 3:24 PM
To: Bernard Tremblay (Bernard.Tremblay@rcmp-grc.gc.ca); [redacted] Carole Smith;

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Pentland, Douglas: CB-BC; Kofler, Gernot: CB-BC; Foley, Lisa: ECOM-DGCE; 'matthew.shogilev@justice.gc.ca' (matthew.shogilev@justice.gc.ca); 'Karen Audcent (Karen.Audcent@justice.gc.ca)'
Cc: Scott, Marcie
Subject: For review - Q&A on number of BSI requests

Colleagues,

Further to the information below, PS has developed a short Q&A answering the question of how many BSI requests are made annually. I would be grateful if you could review the attachment in general and for statistical accuracy regarding your respective organization's BSI figures, by **Monday 16 April**.

Our intent is not to release this information right away, but to have it used at a future date by the minister in a public setting. As such, it will be used publicly at some point.

Thanks,
Maciek

-----Original Message-----
From: Kingsley, Michèle
Sent: March-20-12 10:11 AM
To: Bernard Tremblay
Cc: MacDonald, Michael; Kwavnick, Andrea; Scott, Marcie; Hawrylak, Maciek; Durand, Mathieu; Kousha, Hasti; Audcent, Karen;
Subject: FW: Michael Geist - Halifax Police on Refusals to Provide Subscriber Data: None

Bernard,

Voir l'échange ci-dessous, qui commence avec un rapport de Michael Geist selon quoi certaines forces policières n'ont pas de documentation démontrant le refus de renseignements de bases sur les abonnés. Pas surprenant, puisqu'on ne documente pas les demandes verbales et les refus verbaux...

s.21(1)(b)

the same would be needed from CSIS.

How are we coming along with developing more interception challenge examples? Any more BSI examples?

Merci, Michèle

-----Original Message-----
From: Kingsley, Michèle
Sent: March-20-12 9:39 AM
To: Paulson, Erika; Spendlove, Jim; Joan Butcher (JButcher@justice.gc.ca); Burton, Meredith; Filipps, Lisa; Glazer, David; 'Greg.Scott@bc-cb.gc.ca'; Hawrylak, Maciek; Kousha, Hasti; Kwavnick, Andrea; Lauzon, Adam; Miller, Kevin; PSMediaCentre/CentredesmediasdeSP; Scott, Marcie; Willey, Chris; Wilson, Barbara
Subject: RE: Michael Geist - Halifax Police on Refusals to Provide Subscriber Data: None

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Thanks Erika.

Andrea will send an examples document that had been developed the week of tabling.

As background to what Mr. Geist is writing, authorities often do not have evidence of non-compliance due to the nature of the current voluntary system. To illustrate, a policy officer can ask for the information - if he/she doesn't get it, the negative response doesn't get recorded. The voluntary process is verbal. In some areas of the country, police officers don't bother asking for BSI anymore because of years of refusals from TSPs - that doesn't get recorded. In other areas, police obtain it voluntarily due to a cooperative relationship with the TSP - that doesn't get recorded either.

What's being proposed under C-30 would mandate authorities to determine - and audit - exactly what is being requested, what is being provided, and why. The findings of those audits would be reported. The Privacy Commissioner and other privacy oversight bodies could then audit those requests as well.

If you think turning the above into a response bullet of some kind please let me know.

Merci, Michèle

Michèle Kingsley
Director, Investigative Technologies and Telecommunications Policy | Directrice, Technologies d'enquêtes et politiques des télécommunications National Security Operations | Opérations de la sécurité nationale Public Safety Canada | Sécurité publique Canada
613.949.3181 / michele.kingsley@ps-sp.gc.ca

-----Original Message-----
From: Paulson, Erika
Sent: March-19-12 12:56 PM
To: Spendlove, Jim; [redacted] Joan Butcher (JButcher@justice.gc.ca); Burton, Meredith; Filipps, Lisa; Glazer, David; 'Greg.Scott@bc-cb.gc.ca'; Hawrylak, Maciek; Kingsley, Michèle; Kousha, Hasti; Kwavnick, Andrea; Lauzon, Adam; Maillé, Marie Anick; Miller, Kevin; PSMediaCentre/CentredesmediasdeSP; Scott, Marcie; Willey, Chris; Wilson, Barbara
Subject: FYI: Michael Geist - Halifax Police on Refusals to Provide Subscriber Data: None

FYI - Geist has begun publishing results from his inquiries to local police forces RE non-compliance for voluntary disclosure of BSI by TSPs. According to his recent post, neither Montreal nor Halifax police have evidence of non-compliance. Please find the full article below.

We have a document that provides 5 examples of non-compliance that compromised an investigation, but some are old. Please find it attached. If there are more recent examples/more extensive data on non-compliance for voluntary disclosure, it would prove useful.

Relevant approved MLs are as follows:

- Basic subscriber information is often required at the early stages of investigations and is essential for pursuing investigative leads. The inability to obtain this information in a timely fashion can delay or block important investigations and undermine public safety and security.
- Police also need basic subscriber information for non-investigative purposes. For example, contacting next of kin, returning stolen property or assisting individuals in distress.
- Current federal legislation allows telecommunications service providers to release basic subscriber information to authorities without a warrant. However, they are not required to do so.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- While some service providers do release basic subscriber information to authorities upon request, others fail to provide it in a timely fashion, and others request a warrant. As a result, there is no consistency or predictability across the country when authorities request this basic information and investigations are often delayed or hampered.

Cheers,
Erika Paulson
Tel: 613-993-4415 | BB: [redacted] s.19(1)

*****

FULL ARTICLE:
http://www.michaelgeist.ca/content/view/6382/125/

Halifax Police on Refusals to Provide Subscriber Data: None

Monday March 19, 2012

Among the government's primary justifications for its lawful access/online surveillance bill (Bill C-30) is that since Internet providers have not been required to disclose subscriber information during an investigation, their assistance is inconsistent. For example, the Public Safety backgrounder on the bill states:

Basic subscriber information is often required at the early stages of investigations or to fulfill general policing duties. This information can already be provided without a warrant under existing legislation, but only on a voluntary basis, which results in inconsistent access and delay.

RCMP data indicates that ISPs complied with nearly 95 percent of requests in 2010, suggesting that non-compliance involves a very small number of cases. I recently filed a series of access to information requests with local police forces to better identify whether they were running into problems. The answer so far is no. The request asked for "a list of all incidents since January 1, 2009 where a request to an Internet service provider for customer name, address, email address, internet protocol address, or IMEI number was refused." The Montreal Police responded that there were no records on point. The Halifax Police was very cooperative and undertook a detailed search. This is notable since Bell Aliant is sometimes identified as an ISP that seeks court orders for disclosure of subscriber information. The Halifax Police report:

A search was conducted using key words such as Bell (2022), ISP (1703), computer (540), Rogers (530), Eastlink (119), Facebook (107), Telus (96), internet (90), Aliant (66), Bell/Aliant (8), Internet Protocol (1) and Kodoo (no results). A review was undertaken and we could not find a refusal.

I'll report on other results as they come in.

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Hawrylak, Maciek

From: Hawrylak, Maciek
Sent: May-25-12 11:50 AM
To: 'William Beiersdorfer'
Subject: RE: For review - Q&A on number of BSI requests

The deadline was back in April, so any time really.

[redacted]

Maciek

From: William Beiersdorfer [mailto:William.Beiersdorfer@rcmp-grc.gc.ca]
Sent: May-25-12 11:47 AM
To: Hawrylak, Maciek
Subject: RE: For review - Q&A on number of BSI requests

Hello Maciek

When are you hoping to get this by.

s.21(1)(b)

Bill

>>> "Hawrylak, Maciek" <Maciek.Hawrylak@ps-sp.gc.ca> 2012-05-25 11:34 >>>
Sorry, this was supposed to go to Bill!

Maciek

From: Hawrylak, Maciek
Sent: May-25-12 11:33 AM
To: 'Bernard Tremblay'
Subject: RE: For review - Q&A on number of BSI requests

Bill,

[redacted]

Basically, we would need to know how many BSI requests are made by the RCMP on an annual basis, so that we can put together a Q&A on how many BSI requests are submitted across Canada yearly.

Thanks,
Maciek

From: Bernard Tremblay [mailto:Bernard.Tremblay@rcmp-grc.gc.ca]
Sent: April-12-12 5:17 PM
To: Hawrylak, Maciek
Subject: Re: For review - Q&A on number of BSI requests

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Hi Maciek,

s.19(1) [redacted]

Bernie

>>> "Hawrylak, Maciek" <Maciek.Hawrylak@ps-sp.gc.ca> 2012-04-12 15:23 >>>
Colleagues,

Further to the information below, PS has developed a short Q&A answering the question of how many BSI requests are made annually. I would be grateful if you could review the attachment in general and for statistical accuracy regarding your respective organization's BSI figures, by **Monday 16 April**.

Our intent is not to release this information right away, but to have it used at a future date by the minister in a public setting. As such, it will be used publicly at some point.

Thanks,
Maciek

-----Original Message-----
From: Kingsley, Michèle
Sent: March-20-12 10:11 AM
To: Bernard Tremblay
Cc: MacDonald, Michael; Kwavnick, Andrea; Scott, Marcie; Hawrylak, Maciek; Durand, Mathieu; Kousha, Hasti; Audcent, Karen; [redacted]
Subject: FW: Michael Geist - Halifax Police on Refusals to Provide Subscriber Data: None

Bernard,

Voir l'échange ci-dessous, qui commence avec un rapport de Michael Geist selon quoi certaines forces policières n'ont pas de documentation démontrant le refus de renseignements de bases sur les abonnés. Pas surprenant, puisqu'on ne documente pas les demandes verbales et les refus verbaux...

[redacted]

[redacted] the same would be needed from CSIS.

How are we coming along with developing more interception challenge examples? Any more BSI examples?

Merci, Michèle

-----Original Message-----
From: Kingsley, Michèle

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Sent: March-20-12 9:39 AM
To: Paulson, Erika; Spendlove, Jim; [redacted] Joan Butcher (JButcher@justice.gc.ca); Burton, Meredith; Filipps, Lisa; Glazer, David; 'Greg.Scott@bc-cb.gc.ca'; Hawrylak, Maciek; Kousha, Hasti; Kwavnick, Andrea; Lauzon, Adam; Miller, Kevin; PSMediaCentre/CentredesmediasdeSP; Scott, Marcie; Willey, Chris; Wilson, Barbara
Subject: RE: Michael Geist - Halifax Police on Refusals to Provide Subscriber Data: None

Thanks Erika.

Andrea will send an examples document that had been developed the week of tabling.

As background to what Mr. Geist is writing, authorities often do not have evidence of non-compliance due to the nature of the current voluntary system. To illustrate, a policy officer can ask for the information - if he/she doesn't get it, the negative response doesn't get recorded. The voluntary process is verbal. In some areas of the country, police officers don't bother asking for BSI anymore because of years of refusals from TSPs - that doesn't get recorded. In other areas, police obtain it voluntarily due to a cooperative relationship with the TSP - that doesn't get recorded either.

What's being proposed under C-30 would mandate authorities to determine - and audit - exactly what is being requested, what is being provided, and why. The findings of those audits would be reported. The Privacy Commissioner and other privacy oversight bodies could then audit those requests as well.

If you think turning the above into a response bullet of some kind please let me know.

Merci, Michèle

Michèle Kingsley
Director, Investigative Technologies and Telecommunications Policy | Directrice, Technologies d'enquêtes et politiques des télécommunications National Security Operations | Opérations de la sécurité nationale Public Safety Canada | Sécurité publique Canada
613.949.3181 / michele.kingsley@ps-sp.gc.ca

-----Original Message-----
From: Paulson, Erika
Sent: March-19-12 12:56 PM
To: Spendlove, Jim; [redacted] Joan Butcher (JButcher@justice.gc.ca); Burton, Meredith; Filipps, Lisa; Glazer, David; 'Greg.Scott@bc-cb.gc.ca'; Hawrylak, Maciek; Kingsley, Michèle; Kousha, Hasti; Kwavnick, Andrea; Lauzon, Adam; Maillé, Marie Anick; Miller, Kevin; PSMediaCentre/CentredesmediasdeSP; Scott, Marcie; Willey, Chris; Wilson, Barbara
Subject: FYI: Michael Geist - Halifax Police on Refusals to Provide Subscriber Data: None

FYI - Geist has begun publishing results from his inquiries to local police forces RE non-compliance for voluntary disclosure of BSI by TSPs. According to his recent post, neither Montreal nor Halifax police have evidence of non-compliance. Please find the full article below.

We have a document that provides 5 examples of non-compliance that compromised an investigation, but some are old. Please find it attached. If there are more recent examples/more extensive data on non-compliance for voluntary disclosure, it would prove useful.

Relevant approved MLs are as follows:

Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

- Basic subscriber information is often required at the early stages of investigations and is essential for pursuing investigative leads. The inability to obtain this information in a timely fashion can delay or block important investigations and undermine public safety and security.
- Police also need basic subscriber information for non-investigative purposes. For example, contacting next of kin, returning stolen property or assisting individuals in distress.
- Current federal legislation allows telecommunications service providers to release basic subscriber information to authorities without a warrant. However, they are not required to do so.
- While some service providers do release basic subscriber information to authorities upon request, others fail to provide it in a timely fashion, and others request a warrant. As a result, there is no consistency or predictability across the country when authorities request this basic information and investigations are often delayed or hampered.

Cheers,
Erika Paulson
Tel: 613-993-4415 | BB: [redacted] s.19(1)

*****

FULL ARTICLE:
http://www.michaelgeist.ca/content/view/6382/125/

Halifax Police on Refusals to Provide Subscriber Data: None

Monday March 19, 2012

Among the government's primary justifications for its lawful access/online surveillance bill (Bill C-30) is that since Internet providers have not been required to disclose subscriber information during an investigation, their assistance is inconsistent. For example, the Public Safety backgrounder on the bill states:

Basic subscriber information is often required at the early stages of investigations or to fulfill general policing duties. This information can already be provided without a warrant under existing legislation, but only on a voluntary basis, which results in inconsistent access and delay.

RCMP data indicates that ISPs complied with nearly 95 percent of requests in 2010, suggesting that non-compliance involves a very small number of cases. I recently filed a series of access to information requests with local police forces to better identify whether they were running into problems. The answer so far is no. The request asked for "a list of all incidents since January 1, 2009 where a request to an Internet service provider for customer name, address, email address, internet protocol address, or IMEI number was refused." The Montreal Police responded that there were no records on point. The Halifax Police was very cooperative and undertook a detailed search. This is notable since Bell Aliant is sometimes identified as an ISP that seeks court orders for disclosure of subscriber information. The Halifax Police report:

A search was conducted using key words such as Bell (2022), ISP (1703), computer (540), Rogers (530), Eastlink (119), Facebook (107), Telus (96), internet (90), Aliant (66), Bell/Aliant (8), Internet Protocol (1) and Kodoo (no results). A review was undertaken and we could not find a refusal.

I'll report on other results as they come in.