

**Pages 1 to / à 3
are duplicates of
sont des duplicatas des
pages 7 to / à 9**

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,

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 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

Scott, Marcie

From: Chayer, Marie-Helene
Sent: March 4, 2011 4:37 PM
To: Hawrylak, Maciek
Cc: Haeck, Kimberly; Dincoy, Rana; Moshonas, Jennifer; Emmett, Jamie; Thompson, Julie; Kwavnick, Andrea
Subject: RE: Report on 12th Privacy and Security Conference, 17-18 February

Tracking:

Recipient	Read
Hawrylak, Maciek	Read: 04/03/2011 4:38 PM
Haeck, Kimberly	Read: 04/03/2011 4:53 PM
Dincoy, Rana	
Moshonas, Jennifer	
Emmett, Jamie	
Thompson, Julie	Read: 07/03/2011 8:37 AM
Kwavnick, Andrea	

Thanks Maciek.

Guys – please take a look (but don't distribute further).

Marie

From: Hawrylak, Maciek
Sent: February 28, 2011 4:32 PM
To: Chayer, Marie-Helene
Subject: Report on 12th Privacy and Security Conference, 17-18 February

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.

000007

25/11/2011

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 way 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, 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 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

Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Commissaire à la protection de la vie privée du Canada

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél.: (613) 995-8210
Téloc.: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

DEPUTY MINISTER'S OFFICE
PUBLIC SAFETY CANADA
2011 MAR 17 P 9:40
M



MAR - 9 2011

①

Mr. William V. Baker
Deputy Minister
Public Safety Canada
269 Laurier Avenue West
Ottawa, Ontario
K1A 0P8

② L Clairmont

cc. S. Topper
pls prepare reply
for DM by March 31, 11

Seen by the DM
Vu par le SM

MAR 17 2011

Dear Mr. Baker:

As a group, Canada's Privacy Commissioners remain concerned about the government's current lawful access initiative, in particular Bill C-52, the *Investigating and Preventing Criminal Electronic Communications Act*. We held a teleconference on January 18, 2011 to discuss the issue and would like to relay the substance of that dialogue. While we understand the legitimate needs of law enforcement and national security agencies, as well as their challenges in the context of new information technologies, we would like to bring to your attention the following concerns about the absence of limits on the access powers, the wide scope of information required to be collected and provided by telecommunications companies without a warrant and the inadequacy of internal controls and the legislative gaps in the oversight model.

The overall lawful access initiative

Read together, the provisions of Bills C-50, C-51, and C-52 (augmented by changes in Bills C-22 and C-29) would substantially diminish the privacy rights of Canadians. They do so by enhancing the capacity of the state to conduct surveillance and access private information while reducing the frequency and vigour of judicial scrutiny. In essence, they make it easier for the state to subject more individuals to surveillance and scrutiny.

Need to see if response that we can only speak to...

While we understand the need for law enforcement and national security agencies to function effectively in the context of new information technologies, in our view, it would be misleading to suggest that these bills will simply maintain capacity. Taken together, the proposed changes and new powers add significant new capabilities for investigators to track and search and seize digital information about individuals.

It is also noteworthy that at no time have Canadian authorities provided the public with any evidence or reasoning to suggest that CSIS or any other Canadian law enforcement agencies have been frustrated in the performance of their duties as

→ Memo to DM

- issue

- hstry of consultation w Privacy Comm (see / priv (1))

- suggested letter

to potential am

Letter -> new language in memo to DM. Can't offer anything yet.

000010



a result of shortcomings attributable to current law, TSPs or the manner in which they operate. New powers should be demonstrably necessary as well as proportionate. Ultimately, even if Canadian authorities can show investigations are being frustrated in a digital environment, all the various powers that would be granted to address these issues must be subject to rigorous, independent oversight.

We have examples in QAA on civil & law enforcement interception issues

The Investigating and Preventing Criminal Electronic Communications Act (Bill C-52)

Clause 16 gives unrestricted access to subscriber data records held by telecommunications. We are concerned that the proposed powers are not limited in any fashion. The privacy oversight community in Canada has expressed reservations, in a joint resolution by all of Canada's privacy commissioners signed after the original tabling of similar bills in 2009. A copy of this resolution is attached.

-> Not accurate
- Identifiers Used in Bill
- only for designated officials except for emergencies
- only as part of their duties & records
- Bill will standardize access practices

We are concerned that clause 16 of Bill C-52 would give authorities access to a wide scope of personal information without a warrant; for example, unlisted numbers, email account data and IP addresses. The Government itself took the view that this information was sensitive enough to make trafficking in such 'identity information' a *Criminal Code* offence. Many Canadians consider this information sensitive and worthy of protection, which does not fit with the proposed self-authorized access model.

Currently, under section 487.013 of the *Criminal Code*, investigators require judicial authorization to seek client information like name, address or account numbers from a financial institution or commercial entity. As you are aware, clauses 16 and 17 of C-52 provide law enforcement, CSIS, and Competition officials with warrantless access to "subscriber information" held by telecommunications companies. In our view, law enforcement and security agency access to information linking subscribers to devices and devices to subscribers should generally be subject to prior judicial scrutiny accompanied by the appropriate checks and balances.

Need to get Hash's input.

Not always possible to get a warrant

Lack of appropriate oversight

We are also concerned by the oversight model. Clause 20(4) sets out audit powers for the federal Office of the Privacy Commissioner (OPC) which already exists in section 18 of the *Privacy Act*. Without additional resources to the OPC, however, this additional statutory provision does not augment existing oversight.

?



In addition, we believe the auditing and reporting safeguards should be strengthened. In relation to internal audits required under clause 20 (2), the requirement that law enforcement and security agencies report to "the responsible minister of anything arising out of the audit that in their opinion should be brought to the attention of the minister" should be subject to an objective standard. Agencies should be expressly required to report any collection, use or retention practices that do not appear to be necessary to the duty or function for which they were originally obtained.

Thank you
for your
input. These
will be brought to
the Gov attention
during debate.

Respective roles of the federal, provincial and territorial privacy offices

From our perspective, in relation to oversight, perhaps even more problematic is clause 20(6) which creates an obligation for the federal Office of the Privacy Commissioner to "report on the powers that they [public officers] have to conduct audits similar to those referred to in subject clause 20(4) with respect to police services constituted under the laws of their province." While the OPC has jurisdiction over the Royal Canadian Mounted Police, this provision does not adequately address the issue of those municipal or provincial police services that are not subject to the jurisdiction of a provincial or territorial privacy office or the OPC.

Hasti/
Karon.

Nor does the Bill resolve the legislative gap in jurisdictions where privacy officers do not have the powers necessary to audit compliance by provincial and municipal police forces. These gaps are evident in many jurisdictions. While recognizing that the federal Office of the Privacy Commissioner could exercise its audit provisions over the RCMP, this issue still strikes the provincial and territorial commissioners as a significant concern at the local level. Certainly it raises risks for privacy and diminishes the value of meaningful, timely review.

We are also concerned that very few of our organizations have been consulted in this process, particularly given the review role we are being asked to perform, flowing from clause 20 (3)(c). To this end, we would insist that the relevant federal officials reengage with provincial Offices of the Attorney-General or territorial equivalents. This should lead to a more open dialogue with the provincial commissioners on these issues.

?



Conclusion

We have collectively made a number of recommendations in our 2009 resolution for legislators to consider as they approach the individual pieces of legislation involved in the initiative. We believe that there is insufficient justification for the new powers, that other, less intrusive alternatives can be explored and that a focussed, tailored approach is vital. In our view, this balance has not been achieved.

To remedy these shortcomings, we suggest certain gaps need to be addressed. Provincial and territorial privacy officers would ask that the federal Privacy Commissioner, in reporting to Parliament on the adequacy of audit and investigation powers, should also be expressly authorized to report on whether privacy officers consider themselves to have adequate resources to conduct the necessary audits and reviews. As above, the federal government must commit to working with provincial and territorial governments to ensure that all of the relevant privacy officers have sufficient powers and resources.

It is our intention to provide Parliament and the public with further analysis and assistance with respect to the global privacy effect of proposed lawful access legislation. We also believe that the regulatory and reporting aspects of the initiative need to be as open and transparent as possible.

We appreciate your consideration of these concerns.

Sincerely,

A handwritten signature in cursive script that reads "Jennifer Stoddart".

Jennifer Stoddart,
Privacy Commissioner of Canada

signed by F. Work

Frank Work, Q.C.,
Information and Privacy Commissioner of Alberta



signed by E. Denham

Elizabeth Denham,
Information and Privacy Commissioner for British Columbia

signed by I. Hamilton

Irene Hamilton,
Ombudsman for Manitoba

signed by A. Bertrand

Anne E. Bertrand, Q.C.,
Access to Information and Privacy Commissioner of New Brunswick

signed by E. Ring

Ed Ring,
Information and Privacy Commissioner for Newfoundland and Labrador

signed by E. Keenan Bengts

Elaine Keenan Bengts,
Information and Privacy Commissioner for the Northwest Territories and
Information and Privacy Commissioner for Nunavut

signed by D. McCallum

Dulcie McCallum,
Freedom of Information and Protection of Privacy Review Officer for the Province of
Nova Scotia

signed by A. Cavoukian

Ann Cavoukian, Ph.D,
Information and Privacy Commissioner of Ontario



6

signed by M. MacDonald

Maria C. MacDonald,
Information and Privacy Commissioner of Prince Edward Island

signed by J. Chartier

Me Jean Chartier,
Président de la Commission d'accès à l'information du Québec

signed by R.G. Dickson

R. Gary Dickson, Q.C.,
Information and Privacy Commissioner of Saskatchewan

signed by T.A. McPhee

Tracy-Anne McPhee,
Ombudsman and Information and Privacy Commissioner of Yukon

c.c.: Chair, House of Commons Standing Committee on Justice and Human
Rights (JUST)
Chair, House of Commons Standing Committee on Public Safety and National
Security (SECU)

Encl. (1): 2009 Federal/Provincial/Territorial Resolution

**Pages 16 to / à 19
are not relevant
sont non pertinentes**

Hawrylak, Maciek

From: Hawrylak, Maciek
Sent: March 22, 2011 5:10 PM
To: Kousha, Hasti
Subject:
Hasti,

Thanks,
Maciek

Scott, Marcie

From: Chayer, Marie-Helene
Sent: March 22, 2011 6:47 PM
To: MacDonald, Michael
Subject: Re: URGENT: Letter from Privacy Commissioner Stoddard

Ok. We'll wait.

Thanks
Mh

From: MacDonald, Michael
To: Chayer, Marie-Helene
Sent: Tue Mar 22 18:35:32 2011
Subject: Re: URGENT: Letter from Privacy Commissioner Stoddard

Thx. Everything is good in your plan.

The only thing I question is the memo to the Minister. I would wait on this idea, unless specifically advised.

M

From: Chayer, Marie-Helene
To: MacDonald, Michael
Sent: Tue Mar 22 17:51:39 2011
Subject: RE: URGENT: Letter from Privacy Commissioner Stoddard

Great minds think alike. I spoke to Stacey already. The file is already in DMO. We will use of the language in the note for the response to the letter, which is basically a reiteration of the PC's concerns over C-52. In fact, it is the summary of a conference call she had with her provincial counterparts – which share her concerns.

My plan is to send a docket with a draft letter for the DM and a recommendation that we draft a memo to the Minister explaining the issue

Thoughts?

From: MacDonald, Michael
Sent: March 22, 2011 5:45 PM
To: Chayer, Marie-Helene
Subject: Re: URGENT: Letter from Privacy Commissioner Stoddard

Has it gone to the DMO? Can you check tomorrow - and then you may need to talk to Stacey. Is it has not gone; get Stacey to move it. If it has gone; you may consider integrating this into your actions and if you have LC verbally discuss with the DM

What's the contents of the PC letter?

From: Chayer, Marie-Helene
To: MacDonald, Michael
Sent: Tue Mar 22 17:28:51 2011
Subject: RE: URGENT: Letter from Privacy Commissioner Stoddard

Thanks. Already on it...

It is too bad that our note has not come back from the DMO yet...

From: MacDonald, Michael
Sent: March 22, 2011 5:27 PM
To: Chayer, Marie-Helene
Subject: Fw: URGENT: Letter from Privacy Commissioner Stoddard
Importance: High

From: Dupuis, Chantal
To: Johnston, Shannon
Cc: MacDonald, Michael; Coburn, Stacey; Piasko, Ruba; Dupuis, Chantal
Sent: Tue Mar 22 17:01:01 2011
Subject: FW: URGENT: Letter from Privacy Commissioner Stoddard

Bonjour,

Please bring to the attention of Mike; also note that the docket 378547 was sent to you for a reply.

Chantal Dupuis

Policy Coordinator / Coordinatrice de politiques
Office of the Assistant Deputy Minister / Bureau du Sous-ministre adjointe
Emergency Management and National Security Branch / Secteur de la Gestion des mesures d'urgence et de la Sécurité nationale
Public Safety Canada / Sécurité publique Canada

Tel: 613-990-9270

From: Lambert, Louise
To: Clairmont, Lynda; Tupper, Shawn
Cc: Coburn, Stacey; Lannin, Laurie; Dussault, Josée; Duschner, Gabrielle; Donato, Renée
Sent: Tue Mar 22 15:42:38 2011
Subject: Letter from Privacy Commissioner Stoddard

Docket # 378545 & 378547

HEADS-UP

We were informed that they will be posting the joint letter on their Web site in the next 24 hours.

Louise Lambert
Executive Assistant to the Deputy Minister / Adjointe exécutive du Sous-ministre
Public Safety Canada / Sécurité publique Canada
269 Laurier Avenue West / 269, avenue Laurier Ouest
Ottawa ON K1A 0P8
Tel: 613-991-2891 Fax: 613-990-8312

000022

25/11/2011

Hawrylak, Maciek

From: Kousha, Hasti
Sent: March 24, 2011 10:20 AM
To: Hawrylak, Maciek
Subject: RE:
Follow Up Flag: Follow up
Flag Status: Purple
Attachments:

Hi Maciek,

I hope this helps. Let me know if I can be of more assistance.

Thank you,
Hasti

Hasti Kousha
Legal Counsel/Avocate
Public Safety Canada Legal Services/Services juridiques Sécurité publique Canada
269 Laurier Avenue West/269, avenue Laurier Ouest
Ottawa, Ontario
Telephone/Téléphone: 613-949-9927
Facsimile/Télécopieur: 613-990-8307
Email/Courriel: hasti.kousha@ps-sp.gc.ca

SOLICITOR-CLIENT PRIVILEGE/SECRET PROFESSIONNEL DE L'AVOCAT

From: Hawrylak, Maciek
Sent: March 23, 2011 3:55 PM
To: Kousha, Hasti
Subject:
Importance: High

Hasti,

Many thanks,
Maciek

**Pages 26 to / à 30
are withheld pursuant to section
sont retenues en vertu de l'article**

**of the Access to Information
de la Loi sur l'accès à l'information**

Hawrylak, Maciek

From: Paulson, Erika
Sent: March 25, 2011 10:11 AM
To: Hawrylak, Maciek
Cc: Burton, Meredith
Subject: FYI - RE: Release of letter on lawful access from Privacy Commissioner to DM Public Safety
Follow Up Flag: Follow up
Flag Status: Purple
Attachments: PS-SP-#398703-v2-MLs_-_Lawful_Access.DOC

Hi, Maciek. FYI- I've provided my issues management team (who deal with media calls) with November's approved media lines on the LA leg. I updated the tense to reflect the current election climate. Considering all that's going on, it's unlikely to be picked up in the media, but it's best to be prepared and ensure that our messaging, including that in the letter, are consistent. We'd appreciate a look at the letter once you're able.

Cheers,
Erika Paulson
Tel: 613-993-4415

From: Burton, Meredith
Sent: March 24, 2011 7:13 PM
To: Hawrylak, Maciek
Cc: Paulson, Erika
Subject: Re: Release of letter on lawful access from Privacy Commissioner to DM Public Safety

Thanks Maciek. Would it be possible to review the draft letter before it goes to DMO? I don't want to slow down the process, just to verify that the wording is consistent with what we've used before.

Erika, please check the Privacy Commissioner's site tomorrow for that letter. .

From: Hawrylak, Maciek
To: Burton, Meredith
Sent: Thu Mar 24 17:18:08 2011
Subject: Release of letter on lawful access from Privacy Commissioner to DM Public Safety

Meredith,

This is a heads-up to advise you that we recently received a letter from the Privacy Commissioner of Canada re-iterating concerns with respect to Bill C-52 and wider lawful access legislation in general. We were advised yesterday by ADMO that the Commissioner was going to post the letter on her website within 24 hours, which it appears she has done: http://www.priv.gc.ca/media/nr-c/2011/let_110309_e.cfm

We will be sending a draft reply to the letter to the DM early next week. Please let me know if you have any questions.

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

000031

24/11/2011



Media Lines

ISSUE: On November 1, 2010, the Government of Canada introduced Bill C-52, the *Investigating and Preventing Criminal Electronic Communications Act* to support the interception of communications by the police and the Canadian Security Intelligence Service (CSIS) by requiring intercept capability in telecommunications networks. The law will also provide the police, CSIS and the Competition Bureau with basic subscriber information. This legislation had previously been introduced as the *Technical Assistance for Law Enforcement in the 21st Century Act* (formerly Bill C-47).

MEDIA LINES:

- The Government of Canada is committed to the safety and security of Canadians and their communities.
- This legislation was drafted to help keep Canadians safe from those who would use new communications technology to pursue criminal or terrorist activities.
- The *Investigating and Preventing Criminal Electronic Communications Act* was drafted to ensure that law enforcement and CSIS can keep pace with new communication technologies and are able to execute judicially authorized warrants.
- The legislation drafted did not provide new powers to intercept communications. The warrant processes for the interception of private communications will not change with this Bill.
- The legislation was drafted to provide for a balanced and well-regulated administrative regime for the disclosure of basic subscriber information to the police, CSIS and the Competition Bureau when requested.
- Canada drafted this bill to join many other countries including the United Kingdom, the United States, Australia, Germany and Sweden, which already have similar laws to ensure intercept capability and the sharing of basic subscriber information.

If asked about interception:

- This Government is committed to providing law enforcement and national security agencies with the tools they need to prevent, investigate and prosecute serious crimes including terrorism.

- 2 -

- While technology has advanced over the past two decades, the capability of police to lawfully intercept communications has not kept pace.
- Courts will continue to review and authorize requests to intercept communications, as is the case today.

If asked about subscriber information:

- This legislation was drafted to ensure that the police, CSIS and the Competition Bureau will, upon request, be provided basic subscriber 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.
- Rigorous safeguards will be put in place to protect subscriber information.
- This drafted legislation was the result of years of consultations with a wide range of stakeholders including the telecommunications industry, civil liberties groups, victims' advocates, police associations and provincial/territorial justice officials.
- The proposed legislation achieves the necessary balance, taking into account the needs of the police, CSIS and the Competition Bureau, and the privacy rights of Canadians.
- It was drafted to help authorities investigate suspected criminals and terrorists who represent a serious threat to the safety and security of Canada.

If asked why subscriber information does not require a warrant:

- Presently, requesting basic subscriber information such as name or address does not require a warrant.
- The problem is that, while some service providers release basic subscriber information to authorities upon request, others fail to provide it in a timely fashion, and others insist on a warrant. However, in many situations, obtaining a warrant for this basic information is neither practical nor possible.
- This law was drafted to ensure consistency across the country by compelling telecommunications service providers to disclose basic subscriber information to the police, CSIS and the Competition Bureau when requested.
- As part of our consultations, we've heard from authorities about the need for access to basic subscriber information.

- 3 -

- We've heard disturbing stories from the National Child Exploitation Co-ordination Centre about cases they could not pursue due to insufficient information. For example:
 - As part of a massive world wide investigation of child pornography, Germany alerted Canadian law enforcement of 200 Internet Protocol addresses associated with online child sexual exploitation.
 - The RCMP requested information from Internet service providers to identify potential suspects. Unfortunately, 47 of those requests were refused.
 - There was insufficient information in these cases to obtain warrants. That means 47 leads reached a dead-end and countless children remain at risk.
- This proposed legislation was drafted to help to ensure that there are no more dead-end investigations.

Hawrylak, Maciek

From: Burton, Meredith
Sent: March 25, 2011 3:34 PM
To: Hawrylak, Maciek
Cc: Paulson, Erika
Subject: Re: Release of letter on lawful access from Privacy Commissioner to DM Public Safety
Follow Up Flag: Follow up
Flag Status: Purple

That will work very well.
Thanks!

From: Hawrylak, Maciek
To: Burton, Meredith
Cc: Paulson, Erika
Sent: Fri Mar 25 15:27:15 2011
Subject: RE: Release of letter on lawful access from Privacy Commissioner to DM Public Safety

Meredith,

We'd be happy to share it with you before we take it up the chain. I'm not exactly sure when that will be, and unfortunately I won't be able to give you more than one day with it, but I'll be sure to advise you once we're ready.

Regards,
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: Burton, Meredith
Sent: March 24, 2011 7:13 PM
To: Hawrylak, Maciek
Cc: Paulson, Erika
Subject: Re: Release of letter on lawful access from Privacy Commissioner to DM Public Safety

Thanks Maciek. Would it be possible to review the draft letter before it goes to DMO? I don't want to slow down the process, just to verify that the wording is consistent with what we've used before.

Erika, please check the Privacy Commissioner's site tomorrow for that letter. .

From: Hawrylak, Maciek
To: Burton, Meredith
Sent: Thu Mar 24 17:18:08 2011
Subject: Release of letter on lawful access from Privacy Commissioner to DM Public Safety

000035

24/11/2011

Meredith,

This is a heads-up to advise you that we recently received a letter from the Privacy Commissioner of Canada re-iterating concerns with respect to Bill C-52 and wider lawful access legislation in general. We were advised yesterday by ADMO that the Commissioner was going to post the letter on her website within 24 hours, which it appears she has done: http://www.priv.gc.ca/media/nr-c/2011/let_110309_e.cfm

We will be sending a draft reply to the letter to the DM early next week. Please let me know if you have any questions.

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

000036

24/11/2011



Public Safety / Sécurité publique
Canada / Canada

Assistant Deputy Minister / Sous-ministre adjoint

Ottawa, Canada
K1A 0P8

DEPUTY MINISTER'S OFFICE
PUBLIC SAFETY CANADA

2011 APR -4 P 1:55

DEPUTY MINISTER'S OFFICE
PUBLIC SAFETY CANADA

2011 APR -5
UNCLASSIFIED

DATE: **April 1 / 11**

File No.: CR1173-P10 PRO / 378547

RDIMS No.: 399769

MEMORANDUM FOR THE DEPUTY MINISTER

**FEDERAL AND PROVINCIAL PRIVACY COMMISSIONERS'
SUGGESTED AMENDMENTS TO LAWFUL ACCESS LEGISLATION**

(Signature required)

ISSUE

The federal and provincial Privacy Commissioners sent you a letter dated March 9, 2011, reiterating privacy concerns related to the former Bill C-52, *Investigating and Preventing Criminal Electronic Communications Act*, and to suggest possible amendments to the Bill (**TAB A**). Your signature is requested on a response to this letter (**TAB B**).

BACKGROUND

Over the past years, the federal and provincial Privacy Commissioners have highlighted privacy concerns regarding lawful access legislation. In their most recent correspondence of March 9, 2011, they raised the following concerns:

- Bill C-52 will increase the capacity of the state to conduct surveillance while simultaneously reducing judicial oversight;
- there is a lack of evidence suggesting an operational need for the Bill;
- the basic subscriber information component of the Bill is too broad and allows for unrestricted access to this information;
- there is a lack of resources and powers for privacy commissioners to audit the basic subscriber information regime;
- there are jurisdictional issues pertaining to the extent of the powers of some provincial commissioners; and
- there were insufficient consultations on the Bill with the provincial commissioners.

UNCLASSIFIED

- 2 -

Government officials consulted with Privacy Commissioners at the federal and provincial levels on many occasions regarding lawful access legislation. The first consultation occurred in the fall of 2002, at which time officials explained the requirement for such legislation and received input from the federal and provincial Privacy Commissioners. In March 2005, prior to the first introduction of lawful access legislation, Public Safety Canada (PS) officials explained the legislation and discussed the privacy impact of the Bill with the Privacy Commissioners of Canada, Ontario, Alberta, and British Columbia. In August 2007, all Privacy Commissioners were again invited to submit comments on lawful access legislative proposals. You will recall that on December 15, 2011, you met with the federal Privacy Commissioner, Ms. Jennifer Stoddart, to discuss the most recent iteration of lawful access legislation, the former Bill C-52. In addition, there have been many bilateral meetings between PS officials and the Office of the Privacy Commissioner in this regard.

CONSIDERATIONS

As Bill C-52 died on the Order Paper with the dissolution of Parliament on March 25, 2011, the proposed response to the Privacy Commissioners (**TAB B**) does not focus on the privacy safeguards built into former Bill C-52, but rather reiterates PS's commitment to balance privacy concerns with investigative needs. PS officials continue to look at ways to address some of the Privacy Commissioners' concerns in a subsequent iteration of lawful access legislation, and will soon engage PS portfolio agencies to discuss potential options.

RECOMMENDATION

It is recommended that you sign the enclosed letter to the Privacy Commissioners, addressing PS's commitment to balance privacy concerns with investigative needs.

Should you require additional information, please do not hesitate to contact me or Michael MacDonald, Director General, National Security Operations, at 613-993-4595.



Lynda Clairmont
Assistant Deputy Minister
Emergency Management and National Security

Enclosures: (2)

Prepared by: Maciek Hawrylak

000038

Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél.: (613) 995-8210
Télec.: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

DEPUTY MINISTER'S OFFICE
PUBLIC SAFETY CANADA
2011 MAR 17 P 9:40
M



MAR - 9 2011

① Mr. William V. Baker
Deputy Minister
Public Safety Canada
269 Laurier Avenue West
Ottawa, Ontario
K1A 0P8

② L Clairmont
cc. S. Topper
pls prepare reply
for DM by March 31, 11

Seen by the DM
Vu par le SM

MAR 17 2011

Dear Mr. Baker:

As a group, Canada's Privacy Commissioners remain concerned about the government's current lawful access initiative, in particular Bill C-52, the *Investigating and Preventing Criminal Electronic Communications Act*. We held a teleconference on January 18, 2011 to discuss the issue and would like to relay the substance of that dialogue. While we understand the legitimate needs of law enforcement and national security agencies, as well as their challenges in the context of new information technologies, we would like to bring to your attention the following concerns about the absence of limits on the access powers, the wide scope of information required to be collected and provided by telecommunications companies without a warrant and the inadequacy of internal controls and the legislative gaps in the oversight model.

The overall lawful access initiative

Read together, the provisions of Bills C-50, C-51, and C-52 (augmented by changes in Bills C-22 and C-29) would substantially diminish the privacy rights of Canadians. They do so by enhancing the capacity of the state to conduct surveillance and access private information while reducing the frequency and vigour of judicial scrutiny. In essence, they make it easier for the state to subject more individuals to surveillance and scrutiny.

While we understand the need for law enforcement and national security agencies to function effectively in the context of new information technologies, in our view, it would be misleading to suggest that these bills will simply maintain capacity. Taken together, the proposed changes and new powers add significant new capabilities for investigators to track and search and seize digital information about individuals.

It is also noteworthy that at no time have Canadian authorities provided the public with any evidence or reasoning to suggest that CSIS or any other Canadian law enforcement agencies have been frustrated in the performance of their duties as

.../2



a result of shortcomings attributable to current law, TSPs or the manner in which they operate. New powers should be demonstrably necessary as well as proportionate. Ultimately, even if Canadian authorities can show investigations are being frustrated in a digital environment, all the various powers that would be granted to address these issues must be subject to rigorous, independent oversight.

The Investigating and Preventing Criminal Electronic Communications Act (Bill C-52)

Clause 16 gives unrestricted access to subscriber data records held by telecommunications. We are concerned that the proposed powers are not limited in any fashion. The privacy oversight community in Canada has expressed reservations, in a joint resolution by all of Canada's privacy commissioners signed after the original tabling of similar bills in 2009. A copy of this resolution is attached.

We are concerned that clause 16 of Bill C-52 would give authorities access to a wide scope of personal information without a warrant; for example, unlisted numbers, email account data and IP addresses. The Government itself took the view that this information was sensitive enough to make trafficking in such 'identity information' a *Criminal Code* offence. Many Canadians consider this information sensitive and worthy of protection, which does not fit with the proposed self-authorized access model.

Currently, under section 487.013 of the *Criminal Code*, investigators require judicial authorization to seek client information like name, address or account numbers from a financial institution or commercial entity. As you are aware, clauses 16 and 17 of C-52 provide law enforcement, CSIS, and Competition officials with warrantless access to "subscriber information" held by telecommunications companies. In our view, law enforcement and security agency access to information linking subscribers to devices and devices to subscribers should generally be subject to prior judicial scrutiny accompanied by the appropriate checks and balances.

Lack of appropriate oversight

We are also concerned by the oversight model. Clause 20(4) sets out audit powers for the federal Office of the Privacy Commissioner (OPC) which already exists in section 18 of the *Privacy Act*. Without additional resources to the OPC, however, this additional statutory provision does not augment existing oversight.



In addition, we believe the auditing and reporting safeguards should be strengthened. In relation to internal audits required under clause 20 (2), the requirement that law enforcement and security agencies report to “the responsible minister of anything arising out of the audit that in their opinion should be brought to the attention of the minister” should be subject to an objective standard. Agencies should be expressly required to report any collection, use or retention practices that do not appear to be necessary to the duty or function for which they were originally obtained.

Respective roles of the federal, provincial and territorial privacy offices

From our perspective, in relation to oversight, perhaps even more problematic is clause 20(6) which creates an obligation for the federal Office of the Privacy Commissioner to “report on the powers that they [public officers] have to conduct audits similar to those referred to in subject clause 20(4) with respect to police services constituted under the laws of their province.” While the OPC has jurisdiction over the Royal Canadian Mounted Police, this provision does not adequately address the issue of those municipal or provincial police services that are not subject to the jurisdiction of a provincial or territorial privacy office or the OPC.

Nor does the Bill resolve the legislative gap in jurisdictions where privacy officers do not have the powers necessary to audit compliance by provincial and municipal police forces. These gaps are evident in many jurisdictions. While recognizing that the federal Office of the Privacy Commissioner could exercise its audit provisions over the RCMP, this issue still strikes the provincial and territorial commissioners as a significant concern at the local level. Certainly it raises risks for privacy and diminishes the value of meaningful, timely review.

We are also concerned that very few of our organizations have been consulted in this process, particularly given the review role we are being asked to perform, flowing from clause 20 (3)(c). To this end, we would insist that the relevant federal officials reengage with provincial Offices of the Attorney-General or territorial equivalents. This should lead to a more open dialogue with the provincial commissioners on these issues.

.../4



Conclusion

We have collectively made a number of recommendations in our 2009 resolution for legislators to consider as they approach the individual pieces of legislation involved in the initiative. We believe that there is insufficient justification for the new powers, that other, less intrusive alternatives can be explored and that a focussed, tailored approach is vital. In our view, this balance has not been achieved.

To remedy these shortcomings, we suggest certain gaps need to be addressed. Provincial and territorial privacy officers would ask that the federal Privacy Commissioner, in reporting to Parliament on the adequacy of audit and investigation powers, should also be expressly authorized to report on whether privacy officers consider themselves to have adequate resources to conduct the necessary audits and reviews. As above, the federal government must commit to working with provincial and territorial governments to ensure that all of the relevant privacy officers have sufficient powers and resources.

It is our intention to provide Parliament and the public with further analysis and assistance with respect to the global privacy effect of proposed lawful access legislation. We also believe that the regulatory and reporting aspects of the initiative need to be as open and transparent as possible.

We appreciate your consideration of these concerns.

Sincerely,

Jennifer Stoddart,
Privacy Commissioner of Canada

signed by F. Work

Frank Work, Q.C.,
Information and Privacy Commissioner of Alberta



5

signed by E. Denham

Elizabeth Denham,
Information and Privacy Commissioner for British Columbia

signed by I. Hamilton

Irene Hamilton,
Ombudsman for Manitoba

signed by A. Bertrand

Anne E. Bertrand, Q.C.,
Access to Information and Privacy Commissioner of New Brunswick

signed by E. Ring

Ed Ring,
Information and Privacy Commissioner for Newfoundland and Labrador

signed by E. Keenan Bengts

Elaine Keenan Bengts,
Information and Privacy Commissioner for the Northwest Territories and
Information and Privacy Commissioner for Nunavut

signed by D. McCallum

Dulcie McCallum,
Freedom of Information and Protection of Privacy Review Officer for the Province of
Nova Scotia

signed by A. Cavoukian

Ann Cavoukian, Ph.D,
Information and Privacy Commissioner of Ontario



6

signed by M. MacDonald

Maria C. MacDonald,
Information and Privacy Commissioner of Prince Edward Island

signed by J. Chartier

Me Jean Chartier,
Président de la Commission d'accès à l'information du Québec

signed by R.G. Dickson

R. Gary Dickson, Q.C.,
Information and Privacy Commissioner of Saskatchewan

signed by T.A. McPhee

Tracy-Anne McPhee,
Ombudsman and Information and Privacy Commissioner of Yukon

c.c.: Chair, House of Commons Standing Committee on Justice and Human
Rights (JUST)
Chair, House of Commons Standing Committee on Public Safety and National
Security (SECU)

Encl. (1): 2009 Federal/Provincial/Territorial Resolution

“Protecting Privacy for Canadians in the 21st Century”
Resolution of Canada’s Privacy Commissioners and Privacy Enforcement
Officials on Bills C-46 and C-47
September 9-10, 2009, St. John’s, Newfoundland and Labrador

CONTEXT

1. The federal government tabled two pieces of legislation in June 2009 aimed at giving Canadian law enforcement, national security agencies and others (hereafter referred to as “authorities”) broader powers to acquire digital evidence to support their investigations.
2. Bill C-46, the Investigative Powers for the 21st Century Act (IP21C), would allow authorities to order telecommunications providers to preserve and turn over the details of their subscribers’ communications. Authorities would also have the power to apply for special orders to trace mobile communications devices and, by extension, their owners.
3. Bill C-47, the Technical Assistance for Law Enforcement in the 21st Century Act (TALEA), would give authorities access to information about subscribers and their mobile devices, even without a warrant. The bill would also oblige all telecommunications companies to build in a capability allowing authorities to intercept communications on their networks.
4. The provisions of the proposed Acts raise privacy concerns. For instance, without a warrant, authorities could gain access to personal information such as unlisted telephone numbers, and e-mail and IP addresses.
5. Canadians consider much of this personal information to be sensitive and expect it to be kept confidential.
6. Canadians also expect their use of computers and mobile devices to remain private.
7. The legislation as currently drafted is not limited only to investigations of serious criminal offences, but also could be used to target even minor infractions and non-criminal matters.

WHEREAS

1. Privacy is a fundamental human right that enables the freedom of association, thought and expression.
2. Canadian courts have consistently affirmed the importance of these rights.
3. Canada has a legal regime governing the use of surveillance that protects individual rights while also giving authorities access to communications when authorized. This framework has been carefully refined over decades by Parliament and the courts.
4. To date, the federal government has presented no compelling evidence that new powers are needed.

THEREFORE

The Federal, Provincial and Territorial Privacy Commissioners of Canada urge Parliament to ensure that the proposed legislation to create an expanded surveillance regime strikes the right balance between individual privacy and the legitimate needs of the authorities by:

1. Approaching IP21C and TALEA with caution because they alter a carefully constructed and workable framework;
2. Obliging the government to demonstrate that the expanded surveillance powers they contain are essential and that each of the new investigative powers is justified;
3. Exploring the alternative that, should these powers be granted, they be limited to dealing with specific, serious crimes and life-threatening emergencies;
4. Ensuring that any legislative proposals on surveillance:
 - a. Be minimally intrusive;
 - b. Impose limits on the use of new powers and ensure appropriate legal thresholds remain in place for court authorization;
 - c. Require that draft regulations be reviewed publicly before coming into force;
 - d. Include effective oversight;
 - e. Provide for regular public reporting on the use of powers; and
 - f. Include a five-year Parliamentary review.



Public Safety Sécurité publique
Canada Canada

Deputy Minister Sous-ministre

Ottawa, Canada
K1A 0P8

AVR
APR - 5 2011

Ms. Jennifer Stoddart
Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario K1A 1H3


Dear Ms. Stoddart:

Thank you for your letter of March 9, 2011, regarding the former Bill C-52, *Investigating and Preventing Criminal Electronic Communications Act*. Public Safety Canada takes the privacy implications of any legislative proposal seriously, and carefully considers the input provided by key stakeholders such as yourself.

As you are aware, Bill C-52 died on the Order Paper on March 25, 2011. We cannot be certain as to the intentions of the next Government, and therefore cannot speculate on the likelihood of the re-introduction of similar legislation. Nevertheless, the need for lawful access legislation has been clearly demonstrated by national security and law enforcement agencies across the country and we fully appreciate the need to strike the right balance between the privacy of Canadians and the investigative and policing requirements. On this point, I think that our last meeting was most fruitful and I have asked my officials to look into options to further protect Canadians' privacy rights. Your suggestions will inform our advice to the next Government on a potential new iteration of lawful access legislation.

I look forward to our continued cooperation and thank you again for your correspondence on this important matter.

Sincerely,



William V. Baker

c.c.: Mr. Frank Work, Q.C.,
Information and Privacy Commissioner of Alberta

Ms. Elizabeth Denham
Information and Privacy Commissioner for British Columbia

Ms. Irene Hamilton
Ombudsman for Manitoba

Canada

Mme. Anne E. Bertrand, Q.C.,
Access to Information and Privacy Commissioner of New Brunswick

Mr. Ed Ring
Information and Privacy Commissioner for Newfoundland and Labrador

Ms. Elaine Keenan Bengts
Information and Privacy Commissioner for the Northwest Territories and
Information and Privacy Commissioner for Nunavut

Ms. Dulcie McCallum
Freedom of Information and Protection of Privacy Review Officer for the
Province of Nova Scotia

Ms. Ann Cavoukian, Ph.D,
Information and Privacy Commissioner of Ontario

Ms. Maria C. MacDonald
Information and Privacy Commissioner of Prince Edward Island

Me Jean Chartier
Président de la Commission d'accès à l'information du Québec

Mr. R. Gary Dickson, Q.C.,
Information and Privacy Commissioner of Saskatchewan

Ms. Tracy-Anne McPhee
Ombudsman and Information and Privacy Commissioner of Yukon

MacDonald, Michael

From: Hawrylak, Maciek
Sent: April-07-11 12:18 PM
To: Coburn, Stacey
Cc: Moshonas, Jennifer; MacDonald, Michael; Johnston, Shannon
Subject: RE: Response to PEI Priv Com Letter Mar 2011 v3 (DG Approved)

Yes.

Maciek

From: Coburn, Stacey
Sent: April 7, 2011 12:18 PM
To: Hawrylak, Maciek
Cc: Moshonas, Jennifer; MacDonald, Michael; Johnston, Shannon
Subject: RE: Response to PEI Priv Com Letter Mar 2011 v3 (DG Approved)

Thank you very much.

Is this DG approved?

Stacey Coburn
949-4490

From: Hawrylak, Maciek
Sent: Thursday, April 07, 2011 12:06 PM
To: Coburn, Stacey
Cc: Moshonas, Jennifer; MacDonald, Michael; Johnston, Shannon
Subject: RE: Response to PEI Priv Com Letter Mar 2011 v3 (DG Approved)

Stacey,

Please find attached the revised version of the letter responding to the PEI Privacy Commissioner, addressing Lynda's comments. I believe you may need to break it across two pages to account for word mark spacing, but otherwise it should be good to go.

Regards,
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: Coburn, Stacey
Sent: April 6, 2011 3:26 PM
To: MacDonald, Michael
Subject: Response to PEI Priv Com Letter Mar 2011 v3 (DG Approved)

Page 50
is a duplicate of
est un duplicata de la
page 58



Public Safety Sécurité publique
Canada Canada

Assistant Deputy Sous-ministre
Minister adjoint

Ottawa, Canada
K1A 0P8

DEPUTY MINISTER'S OFFICE
PUBLIC SAFETY CANADA
UNCLASSIFIED
2011 APR -8 P 12: 19

DATE: APR 08 2011

File No.: ~~CP1173 P10 PRO/~~ 378877

MEMORANDUM FOR THE DEPUTY MINISTER

**PRINCE EDWARD ISLAND PRIVACY COMMISSIONER'S
CONCERNS WITH LAWFUL ACCESS LEGISLATION**

(Signature required)

ISSUE

A proposed response to the Information and Privacy Commissioner of Prince Edward Island's recent correspondence highlighting her lack of a mandate to perform auditing functions related to the basic subscriber information regime in former Bill C-52, the *Investigating and Preventing Criminal Electronic Communications Act* (**TAB 1**).

BACKGROUND

This letter follows a previous letter that the federal and provincial Privacy Commissioners of Canada sent you, dated March 9, 2011, to underscore continued privacy concerns regarding lawful access legislation. The Information and Privacy Commissioner of Prince Edward Island, Maria C. MacDonald, has since sent you a comprehensive letter detailing additional concerns related to her lack of a provincial mandate to audit Prince Edward Island's police forces' compliance with the provisions set out in sections 16 and 17 of former Bill C-52. These sections would have compelled telecommunications service providers to provide basic subscriber information to police, the Canadian Security Intelligence Service, and Competition Bureau officers upon request.

Ms. MacDonald notes in her letter that in Prince Edward Island there is no public officer with powers to oversee the privacy protections established by municipal or university police services. In Ms. MacDonald's view, this creates a gap in the oversight provisions of former Bill C-52 with respect to law enforcement requesting basic subscriber information.

CONSIDERATIONS

Former Bill C-52 did not ascribe auditing powers to provincial privacy commissioners precisely because of a lack of such a mandate in some provinces across Canada. Instead,

.../2

Canada

UNCLASSIFIED

reports on internal audits conducted by provincial or municipal police were to be forwarded by heads of police services directly to the Minister responsible for policing in each province. In the case of Prince Edward Island, this would have been the Minister of Justice and Public Safety and Attorney General. It is this Minister who would have been responsible for ensuring that any Prince Edward Island police force met the statutory provisions related to requests for basic subscriber information under sections 16 and 17 of the former Bill C-52. Heads of police services would also have been required to forward the same report to the provincial privacy commissioner.

In recognition of the fact that some provincial privacy commissioners may not have auditing powers over police services in their province, section 20(6) of former Bill C-52 would have mandated the Privacy Commissioner of Canada to report annually on the powers that provincial privacy commissioners have with respect to auditing police forces in their province. This was designed to allow the Privacy Commissioner of Canada to draw attention to any gaps in powers held by provincial counterparts. Ms. MacDonald's letter demonstrates that these gaps are currently present in Prince Edward Island.

The proposed response (**TAB 2**) acknowledges the unfortunate challenge presented by the lack of consistent mandates with respect to audit powers for provincial privacy commissioners. It also notes that, in light of the fact that Bill C-52 died on the order paper upon the dissolution of Parliament, Public Safety Canada is limited in the extent to which it can commit to further exploring the issues raised in Ms. MacDonald's letter.

RECOMMENDATION

It is recommended that you send the attached letter (**TAB 2**).

Should you require additional information, please do not hesitate to contact me at (613) 990-4976, or Michael MacDonald, Director General, National Security Operations Directorate, at (613) 993-4595.



Lynda Clairmont
Assistant Deputy Minister
Emergency Management and National Security

Enclosures: (2)

Prepared by: Maciek Hawrylak

Prince Edward Island Île-du-Prince-Édouard

Legislative Assembly

Assemblée législative

Seen by the DM
Vu par le SM



Information and
Privacy Commissioner
PO Box 2000, Charlottetown PE
Canada C1A 7N8

Commissaire à l'information et
à la protection de la vie privée
C.P. 2000, Charlottetown PE
Canada C1A 7N8

MAR 31 2011

March 18, 2011

DEPUTY MINISTER'S
PUBLIC SAFETY CANADA

2011 MAR 30 P 3:12

M

RECORDS MANAGEMENT GESTION DES DOCUMENTS
Send To: Envoyez à: DMO
File Number: No de dossier: A-1173-PI0
Temp Docket No: No dossier temp: 378877
File location: Dossier avec:
Control No: No de contrôle:

Reçu
Sécurité publique
Canada

2011 MAR 30 AM 8:52

Received
Public Safety Canada

①

William V. Baker, Deputy Minister
Public Safety Canada
269 Laurier Avenue, West
Ottawa, ON
K1A 0P8

② Lynda Clairmont

Dear Mr. Baker:

Re: Bill C-52, "An Act Regulating Telecommunication Facilities to Support Investigations"

I am joining my name and support with other Information and Privacy Commissioners of Canada in a joint letter setting out several concerns about Bill C-52 "An Act regulating telecommunication facilities to support investigations". I write this separate letter to explain another concern that would not necessarily affect the other jurisdictions. On PEI there is a gap in the oversight provisions of Bill C-52.

Clause 20 of Bill C-52 requires regular audits of the practices of a particular group of users. If an audit reveals a concern and if the auditor considers this issue to be of interest to the Minister responsible for that group of users, the Auditor reports this finding to the Minister. If a report is created for the Minister, a copy of that audit report is also provided to the public officer for that province whose duties include investigations relating to the protection of privacy. We have a few police bodies that are designated under our provincial legislation: municipal forces for Charlottetown, Summerside, Borden-Carleton and Kensington; and the security police officers on the University and College campuses. In PEI there is no public officer with powers to oversee the protection of privacy by municipal police or university/campus police. The Information and Privacy Commissioner does not have jurisdiction over the university, college, or municipal police forces nor does the federal Privacy Commissioner. Generally speaking, the federal PIPEDA, does not apply to municipalities and universities because they are not engaged in trade and commerce.

The *Freedom of Information and Protection of Privacy Act* applies to the provincial government and a list of agencies, boards, commissions and corporations designated as a public body in the regulations. I am not aware of any plans of the Legislature to amend the Regulations to add the

university, college, municipal governments or municipal police to the enumerated bodies which are subject to the *Act*. Nor am I aware of any plans to enact municipal privacy legislation, or amend the Acts that govern the University or College to create a public officer responsible for privacy. I expect I would be consulted if any of these legislative changes were in the works.

Please feel free to contact me with any questions or comments you may have with regard to the content of this letter.

Sincerely,



Maria C. MacDonald
Information and Privacy Commissioner

MCM/ms
enclosure

cc: The Honourable Catherine S. Callbeck, Senator
The Honourable Percy E. Downe, Senator
The Honourable Michael Duffy, Senator
The Honourable Elizabeth Hubley, Senator

The Honourable Wayne Easter, PC, MP
The Honourable Lawrence MacAulay, PC, MP
The Honourable Shawn Murphy, PC, MP
The Honourable Gail Shea, PC, MP, Minister of Fisheries and Oceans

Jennifer Stoddard, Privacy Commissioner of Canada

2010

Enquêtes visant les communications électroniques criminelles et leur prévention

13

Internal audit

20. (1) The Commissioner of the Royal Canadian Mounted Police, the Director of the Canadian Security Intelligence Service, the Commissioner of Competition and any chief or head of a police service constituted under the laws of a province who makes a designation under subsection 16(3) must cause internal audits to be regularly conducted of the practices of his or her agency to ensure compliance with sections 16 to 19 and the regulations made for the purposes of those sections and of the internal management and information systems and controls concerning requests made under sections 16 and 17.

20. (1) Le commissaire de la Gendarmerie royale du Canada, le directeur du Service canadien du renseignement de sécurité, le commissaire de la concurrence ou le chef ou directeur d'un service de police constitué sous le régime d'une loi provinciale qui a fait la désignation prévue au paragraphe 16(3) fait procéder régulièrement, d'une part, à des vérifications internes des méthodes et usages de son organisme afin de contrôler l'observation des articles 16 à 19 et de leurs règlements d'application et, d'autre part, à des vérifications internes des moyens de contrôle et des systèmes en matière de gestion et d'information concernant les demandes prévues aux articles 16 et 17.

Vérification interne

Report to responsible minister

(2) The person who causes an internal audit to be conducted must, without delay, make a report to the responsible minister of anything arising out of the audit that in his or her opinion should be brought to the attention of that minister including any corrective action proposed or taken.

(2) La personne qui fait procéder à une vérification interne établit dans les meilleurs délais à l'intention du ministre compétent un rapport sur toute question découlant de la vérification qui, à son avis, doit être portée à la connaissance de celui-ci, y compris les mesures de redressement prises ou proposées.

Rapport au ministre

Copy of report

(3) A copy of the report is to be provided by that person

(3) Elle transmet une copie du rapport :

Copie du rapport

(a) if it concerns the Royal Canadian Mounted Police or the Commissioner of Competition, to the Privacy Commissioner appointed under section 53 of the *Privacy Act*;

a) si celui-ci est établi par le commissaire de la Gendarmerie royale du Canada ou le commissaire de la concurrence, au Commissaire à la protection de la vie privée nommé en vertu de l'article 53 de la *Loi sur la protection des renseignements personnels*;

(b) if it concerns the Canadian Security Intelligence Service, to the Security Intelligence Review Committee established by subsection 34(1) of the *Canadian Security Intelligence Service Act*; and

b) s'il est établi par le directeur du Service canadien du renseignement de sécurité, au comité de surveillance des activités de renseignement de sécurité constitué par le paragraphe 34(1) de la *Loi sur le Service canadien du renseignement de sécurité*;

(c) if it concerns a police service constituted under the laws of a province, to the public officer for that province whose duties include investigations relating to the protection of privacy.

c) s'il est établi par le chef ou directeur d'un service de police constitué sous le régime d'une loi provinciale, au fonctionnaire de la province dont les fonctions comportent les enquêtes relatives à la protection de la vie privée.



Audit — Privacy Commissioner

(4) The Privacy Commissioner may, on reasonable notice, conduct an audit of the practices of the Royal Canadian Mounted Police or the Commissioner of Competition to ensure compliance with sections 16 to 19 and the regulations made for the purposes of those

(4) Le Commissaire à la protection de la vie privée peut, sur préavis suffisant, procéder, d'une part, à des vérifications des méthodes et usages de la Gendarmerie royale du Canada ou du commissaire de la concurrence afin de contrôler l'observation des articles 16 à 19 et

Vérification: Commissaire à la protection de la vie privée

From Bill C-52
"An Act Regulating
Telecommunications Facilities
to Support Investigations."

Investigating and Preventing Criminal Electronic Communications

sections and of the internal management and information systems and controls concerning requests made under sections 16 and 17. The provisions of the *Privacy Act* apply, with any necessary modifications, in respect of the audit as if it were an investigation under that Act.

de leurs règlements d'application et, d'autre part, à des vérifications des moyens de contrôle et des systèmes en matière de gestion et d'information de l'un ou l'autre concernant les demandes prévues aux articles 16 et 17. La *Loi sur la protection des renseignements personnels* s'applique, avec les adaptations nécessaires, à la vérification comme si elle constituait une enquête en vertu de cette loi.

Audit — Security Intelligence Review Committee

(5) For greater certainty, the functions of the Security Intelligence Review Committee under section 38 of the *Canadian Security Intelligence Service Act* include the power to conduct an audit of the practices of the Canadian Security Intelligence Service to ensure compliance with sections 16, 18 and 19 and the regulations made for the purposes of those sections and of the internal management and information systems and controls concerning requests made under section 16.

(5) Il est entendu que les fonctions du comité de surveillance des activités de renseignement de sécurité prévues à l'article 38 de la *Loi sur le Service canadien du renseignement de sécurité* comportent le pouvoir de procéder aux vérifications des méthodes et usages du Service canadien du renseignement de sécurité afin de contrôler l'observation des articles 16, 18 et 19 et de leurs règlements d'application et aux vérifications des moyens de contrôle et des systèmes en matière de gestion et d'information de celui-ci concernant les demandes prévues à l'article 16.

Vérification : comité de surveillance des activités de renseignement de sécurité

Report concerning provincial audit capability

(6) The Privacy Commissioner must, in the report made to Parliament for each financial year, identify the public officers to whom copies of reports are to be provided under paragraph (3)(c) and report on the powers that they have to conduct audits similar to those referred to in subsection (4) with respect to the police services constituted under the laws of their province.

(6) Le Commissaire à la protection de la vie privée fait état, dans le rapport qu'il présente pour chaque exercice au Parlement, des fonctionnaires à qui des rapports doivent être transmis en application de l'alinéa (3)c) et du pouvoir qu'ils possèdent de procéder à des vérifications semblables à celles visées au paragraphe (4) à l'égard des services de police constitués sous le régime des lois de leur province.

Rapport concernant la vérification faite au niveau provincial.

Records of service provider

(7) A person conducting an internal audit under this section may require a telecommunications service provider to give the person access to any records in the possession or control of the service provider that are relevant to the audit.

(7) Toute personne procédant à une vérification interne au titre du présent article peut exiger de tout télécommunicateur qu'il lui donne accès à tout registre qu'il possède ou dont il dispose qui est pertinent.

Registres des télécommunicateurs

Definition of "responsible minister"

(8) For the purposes of this section, "responsible minister" means

(8) Pour l'application du présent article, « ministre compétent » s'entend :

Définition de « ministre compétent »

(a) in relation to the Commissioner of the Royal Canadian Mounted Police and the Director of the Canadian Security Intelligence Service, the Minister of Public Safety and Emergency Preparedness;

a) s'agissant du commissaire de la Gendarmerie royale du Canada et du directeur du Service canadien du renseignement de sécurité, du ministre de la Sécurité publique et de la Protection civile;

(b) in relation to the Commissioner of Competition, the Minister of Industry; and

b) s'agissant du commissaire de la concurrence, du ministre de l'Industrie;

Enquêtes visant les communications électroniques criminelles et leur prévention

	(c) in relation to the chief or head of a police service constituted under the laws of a province, the Attorney General of that province.	c) s'agissant du chef ou directeur d'un service de police constitué sous le régime d'une loi provinciale, du procureur général de la province.	
Entitlement to fee	21. (1) A telecommunications service provider that provides information to a person under section 16 or 17 is entitled to be paid the prescribed fee for providing the information.	21. (1) Le télécommunicateur qui fournit des renseignements en application des articles 16 ou 17 a le droit de recevoir les droits réglementaires.	5 Droits
Payment of fee by designating authority	(2) If the information is requested by a designated person under section 16, the fee is to be paid by the designating authority.	(2) Si la demande est faite par une personne désignée au titre de l'article 16, les droits sont payés par la personne qui l'a désignée.	Paiement des droits — personne désignée 10
Payment of fee by police service	(3) If the information is requested by a police officer under section 17, the fee is to be paid by the chief or head of the police service that employs the police officer.	(3) Si elle est faite par un officier de police au titre de l'article 17, ils sont payés par le chef ou directeur du service de police de qui relève l'officier.	Paiement des droits — officier de police 15
Preservation of existing authority	22. Nothing in this Act derogates from any other authority under law to obtain the information referred to in subsection 16(1) from a telecommunications service provider.	22. La présente loi n'a pas pour effet de porter atteinte aux pouvoirs de quiconque d'obtenir, en application d'une règle de droit, les renseignements visés au paragraphe 16(1) auprès d'un télécommunicateur.	Précision 20
Deemed nature of information	23. Personal information, as defined in subsection 2(1) of the <i>Personal Information Protection and Electronic Documents Act</i> , that is provided under subsection 16(1) or 17(1) is deemed, for the purposes of subsections 9(2.1) to (2.4) of that Act, to be disclosed under subparagraph 7(3)(c.1)(i) or (ii), and not under paragraph 7(3)(i), of that Act. This section operates despite the other provisions of Part 1 of that Act.	23. Pour l'application des paragraphes 9(2.1) à (2.4) de la <i>Loi sur la protection des renseignements personnels et les documents électroniques</i> , les renseignements personnels au sens du paragraphe 2(1) de cette loi qui sont fournis au titre des paragraphes 16(1) ou 17(1) sont réputés être communiqués au titre des sous-alinéas 7(3)c.1(i) ou (ii) de cette loi et non de son alinéa 7(3)i). Le présent article s'applique malgré les autres dispositions de la partie 1 de la même loi.	Dérogation 30

MISCELLANEOUS PROVISIONS

DISPOSITIONS DIVERSES

Facility and service information	24. (1) A telecommunications service provider must, on the request of a police officer or of an employee of the Royal Canadian Mounted Police or the Canadian Security Intelligence Service, (a) provide the prescribed information relating to the service provider's telecommunications facilities; (b) indicate what telecommunications services the service provider offers to subscribers; and	24. (1) Sur demande de tout officier de police ou employé de la Gendarmerie royale du Canada ou du Service canadien du renseignement de sécurité, le télécommunicateur : a) lui fournit l'information réglementaire se rapportant à ses installations de télécommunication; b) lui indique la nature des services de télécommunication qu'il offre à ses abonnés;	Renseignements sur les installations et les services 35
----------------------------------	---	---	---



Public Safety Sécurité publique
Canada Canada
Deputy Minister Sous-ministre
Ottawa, Canada
K1A 0P8

AVR - 8 2011
APR

Ms. Maria C. MacDonald
Information and Privacy Commissioner of Prince Edward Island
PO Box 2000
Charlottetown, Prince Edward Island C1A 7N8

Dear Ms. MacDonald:

Thank you for your letter dated March 18, 2011, regarding former Bill C-52, the *Investigating and Preventing Criminal Electronic Communications Act*. As you are likely aware, Bill C-52 died on the Order Paper on March 25, 2011. It is difficult at this time to predict if the subsequent Government will choose to re-introduce lawful access legislation, and what form such legislation may take. Nevertheless, we remain committed to working with the next Government, stakeholders such as yourself, industry, and national security and law enforcement agencies in establishing the most appropriate legislative initiative.

The lack of consistent mandates with respect to audit powers for provincial privacy commissioners is an unfortunate challenge. To address this issue in part, former Bill C-52 would have called attention to this inconsistency by requiring the Privacy Commissioner of Canada to detail annually the sometimes limited extent of powers of provincial officers to conduct audits similar to those referred to in s. 20(4) of the former Bill.

I trust that this addresses some of the concerns raised in your letter. I look forward to our continued dialogue and thank you again for your correspondence on this important matter.

Sincerely,

William V. Baker

c.c.: The Honourable Catherine S. Callbeck, Senator

The Honourable Percy E. Downe, Senator

The Honourable Michael Duffy, Senator

Canada

.../2

- 2 -

The Honourable Elizabeth Hubley, Senator

The Honourable Wayne Easter, P.C., M.P.

The Honourable Lawrence MacAulay, P.C., M.P.

The Honourable Shawn Murphy, P.C., M.P.

The Honourable Gail Shea, P.C., M.P.
Minister of Fisheries and Oceans

Jennifer Stoddart, Privacy Commissioner of Canada



Public Safety Sécurité publique

Canada Canada

Deputy Minister Sous-ministre

Ottawa, Canada
K1A 0P8

AVR - 8 2011
APR

Ms. Jennifer Stoddart
Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario K1A 1H3

Dear Ms. Stoddart:

Thank you for your letter of March 9, 2011, regarding the former Bill C-52, *Investigating and Preventing Criminal Electronic Communications Act*. Public Safety Canada takes the privacy implications of any legislative proposal seriously, and carefully considers the input provided by key stakeholders such as yourself.

As you are aware, Bill C-52 died on the Order Paper on March 25, 2011. We cannot be certain as to the intentions of the next Government, and therefore cannot speculate on the likelihood of the re-introduction of similar legislation. Nevertheless, the need for lawful access legislation has been clearly demonstrated by national security and law enforcement agencies across the country and we fully appreciate the need to strike the right balance between the privacy of Canadians and the investigative and policing requirements. On this point, I think that our last meeting was most fruitful and I have asked my officials to look into options to further protect Canadians' privacy rights. Your suggestions will inform our advice to the next Government on a potential new iteration of lawful access legislation.

I look forward to our continued cooperation and thank you again for your correspondence on this important matter.

Sincerely,

William V. Baker

c.c.: Mr. Frank Work, Q.C.,
Information and Privacy Commissioner of Alberta

Ms. Elizabeth Denham
Information and Privacy Commissioner for British Columbia

Ms. Irene Hamilton
Ombudsman for Manitoba

- 2 -

Mme. Anne E. Bertrand, Q.C.,
Access to Information and Privacy Commissioner of New Brunswick

Mr. Ed Ring
Information and Privacy Commissioner for Newfoundland and Labrador

Ms. Elaine Keenan Bengts
Information and Privacy Commissioner for the Northwest Territories and
Information and Privacy Commissioner for Nunavut

Ms. Dulcie McCallum
Freedom of Information and Protection of Privacy Review Officer for the
Province of Nova Scotia

Ms. Ann Cavoukian, Ph.D.,
Information and Privacy Commissioner of Ontario

Ms. Maria C. MacDonald
Information and Privacy Commissioner of Prince Edward Island

Me Jean Chartier
Président de la Commission d'accès à l'information du Québec

Mr. R. Gary Dickson, Q.C.,
Information and Privacy Commissioner of Saskatchewan

Ms. Tracy-Anne McPhee
Ombudsman and Information and Privacy Commissioner of Yukon

000061

**Pages 62 to / à 63
are duplicates of
sont des duplicatas des
pages 70 to / à 71**

Hawrylak, Maciek

From: Hawrylak, Maciek
Sent: April 8, 2011 9:03 AM
To: Moshonas, Jennifer; Dincoy, Rana
Cc: Haeck, Kimberly
Subject: RE: Stakeholder Interaction

Looks fine to me. Just fixed one typo, in red.

Maciek

From: Moshonas, Jennifer
Sent: April 8, 2011 8:53 AM
To: Dincoy, Rana; Hawrylak, Maciek
Cc: Haeck, Kimberly
Subject: FW: Stakeholder Interaction

Good morning,

Here is something that Andrea put together to respond to a request we received with a turnaround time for 10 am this morn. Can you please review and modify or add if required. Can you please let me know by 9.30? THanks.

The original request is:

2. Domestic Partners/Stakeholders

EMNS, LPB and CSP:

- Please provide a list of your key domestic partners/stakeholders (for example, the Canadian Association of Chiefs of Police), as well as a short explanation of how the relationship with each organization is important to advance Public Safety's objectives.

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: Kwavnick, Andrea
Sent: April 7, 2011 3:53 PM
To: Moshonas, Jennifer
Subject: Stakeholder Interaction

000064

24/11/2011

Jen,

Below are a list of Lawful Access partners/stakeholders, with a short explanation of how the relationship with each organization is important to advance PS' objectives.

Let me know if you need anything more.

Thanks
Andrea

Telecommunications Industry

There are hundreds of service providers in Canada, the main ones being Bell, Rogers and Telus. Many service providers are represented by organizations such as the Information Technology Association of Canada (ITAC) and the Canadian Wireless Telecommunications Association (CWTA). In advancing any lawful access legislation, it is important to cooperate with the telecommunications industry. Industry representatives were consulted in 2002, 2005 and 2007. Meetings were also held with industry representatives in 2009 and 2010. In short, service providers have a long history of cooperating with law enforcement in carrying out interceptions, and have indicated that there is common ground between their views and the interception capability component of past iterations of lawful access legislation. Proposed legislation has included mechanisms to provide flexibility for service providers in order to help to minimize costs. That being said, service providers are concerned about various aspects of any legislation, and have indicated a strong desire to provide input into the regulations that would accompany any legislation.

Privacy Advocates

Authorities require timely access to basic subscriber information in order to successfully fulfil their mandates and keep Canadians safe. As such, the requirement for service providers to provide this information to designated authorities has consistently been present in lawful access legislative initiatives. Provincial and Federal Privacy Commissioners have expressed concern with aspects of the subscriber information provisions of the legislation. In particular, there is concern because authorities would not be required to first obtain a warrant in order to access basic subscriber information. Privacy Commissioners were consulted in 2002, 2005 and 2007. Indeed, the 2007 consultations focussed exclusively on the subscriber information elements of the legislation. PS departmental officials met with the Office of the Privacy Commissioner again in 2010. It is important to continue to meet with privacy advocates to ensure that any lawful access legislation would address their concerns.

Police Services

Provincial and municipal police forces support the need for lawful access legislation, and have for many years been calling on the Government to put such legislation in place. Indeed, when former Bill C-52 (lawful access) was introduced in the Parliament in 2010, representatives from the Canadian Association of Chiefs of Police, the Canadian Police Association and the Canadian Association of Police Boards attended a press conference alongside Government Ministers. It is important to maintain relationships with police services across the country in order to ensure that any lawful access legislation would adequately address their concerns. At the same time, it is important to ensure that police services are aware of their obligations under any proposed legislation.

**Pages 66 to / à 68
are duplicates of
sont des duplicatas des
pages 69 to / à 71**

Scott, Marcie

From: Thompson, Julie
Sent: April 8, 2011 9:59 AM
To: Moshonas, Jennifer
Subject: FW: Stakeholder Interaction
Importance: High

Hi Jen, this is Rana - my email server is not working :(

Two more stakeholder groups domestically for us:

Victims Groups: These support having stronger legal tools to prevent crime and protect citizens. Specifically, the Victims Ombudsman and The Canadian Resource Centre for Victims of Crime (a non-government, non-profit advocacy group for victims and survivors of violent crime) are two supporters for lawful access legislation. The Resource Centre has even indicated in writing that the privacy of individuals cannot take precedence over national security threats nor protection of child victims. Victims Groups' public support of Public Safety initiatives have been helpful in explaining the rationale for many Public Safety initiatives in the media.

Provincial Justice Ministers: They are generally supportive of Public Safety's past efforts in the area of lawful interception. Ministers from Alberta and B.C. specifically have written to the Minister of Public Safety indicating support for lawful access legislation. This could potentially facilitate FPT cooperation on other issues of mutual interest.

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

From: Thompson, Julie
Sent: April 8, 2011 9:38 AM
To: Dincoy, Rana
Subject: RE: Stakeholder Interaction

Hi Rana,
Here is a short description for Victims Groups. Before I send it to Jen do you want to add/mdify anything??

VICTIMS GROUPS

Victims groups provide direct assistance to victims across the country as well as advocate for more services and protections for victims and the public. In the past they participated to consultations for lawful access and shared many of the concerns and views expressed by law enforcement representatives.

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

From: Dincoy, Rana
Sent: April 8, 2011 9:02 AM
To: Thompson, Julie
Cc: Moshonas, Jennifer
Subject: Fw: Stakeholder Interaction

Hi
Since you've been working on LA consultation strategy with MHC would you have a look too? Thanks!

From: Moshonas, Jennifer
To: Dincoy, Rana; Hawrylak, Maciek
Cc: Haeck, Kimberly
Sent: Fri Apr 08 08:53:14 2011
Subject: FW: Stakeholder Interaction

Good morning,

Here is something that Andrea put together to respond to a request we received with a turnaround time for 10 am this morn. Can you please review and modify or add if required. Can you please let me know by 9.30? Thanks.

The original request is:

2. Domestic Partners/Stakeholders

EMNS, LPB and CSP:

- Please provide a list of your key domestic partners/stakeholders (for example, the Canadian Association of Chiefs of Police), as well as a short explanation of how the relationship with each organization is important to advance Public Safety's objectives.

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: Kwavnick, Andrea
Sent: April 7, 2011 3:53 PM
To: Moshonas, Jennifer
Subject: Stakeholder Interaction

000070

25/11/2011

Jen,

Below are a list of Lawful Access partners/stakeholders, with a short explanation of how the relationship with each organization is important to advance PS' objectives.

Let me know if you need anything more.

Thanks
Andrea

Telecommunications Industry

There are hundreds of service providers in Canada, the main ones being Bell, Rogers and Telus. Many service providers are represented by organizations such as the Information Technology Association of Canada (ITAC) and the Canadian Wireless Telecommunications Association (CWTA). In advancing any lawful access legislation, it is important to cooperate with the telecommunications industry. Industry representatives were consulted in 2002, 2005 and 2007. Meetings were also held with industry representatives in 2009 and 2010. In short, service providers have a long history of cooperating with law enforcement in carrying out interceptions, and have indicated that there is common ground between their views and the interception capability component of past iterations of lawful access legislation. Proposed legislation has included mechanisms to provide flexibility for service providers in order to help to minimize costs. That being said, service providers are concerned about various aspects of any legislation, and have indicated a strong desire to provide input into the regulations that would accompany any legislation.

Privacy Advocates

Authorities require timely access to basic subscriber information in order to successfully fulfil their mandates and keep Canadians safe. As such, the requirement for service providers to provide this information to designated authorities has consistently been present in lawful access legislative initiatives. Provincial and Federal Privacy Commissioners have expressed concern with aspects of the subscriber information provisions of the legislation. In particular, there is concern because authorities would not be required to first obtain a warrant in order to access basic subscriber information. Privacy Commissioners were consulted in 2002, 2005 and 2007. Indeed, the 2007 consultations focussed exclusively on the subscriber information elements of the legislation. PS departmental officials met with the Office of the Privacy Commissioner again in 2010. It is important to continue to meet with privacy advocates to ensure that any lawful access legislation would address their concerns.

Police Services

Provincial and municipal police forces support the need for lawful access legislation, and have for many years been calling on the Government to put such legislation in place. Indeed, when former Bill C-52 (lawful access) was introduced in the Parliament in 2010, representatives from the Canadian Association of Chiefs of Police, the Canadian Police Association and the Canadian Association of Police Boards attended a press conference alongside Government Ministers. It is important to maintain relationships with police services across the country in order to ensure that any lawful access legislation would adequately address their concerns. At the same time, it is important to ensure that police services are aware of their obligations under any proposed legislation.

Scott, Marcie

From: Brock, Darlene
Sent: April 12, 2011 4:59 PM
To: MacDonald, Michael
Cc: Coburn, Stacey; Moshonas, Jennifer; Chayer, Marie-Helene; Kwavnick, Andrea
Subject: RE: TIME SENSITIVE - Memo to DM - Privacy Commissioner Visit April 14, 2011
Thanks - greatly appreciated.

From: MacDonald, Michael
Sent: Tuesday, April 12, 2011 4:52 PM
To: Brock, Darlene
Cc: Coburn, Stacey; Moshonas, Jennifer; Chayer, Marie-Helene; Kwavnick, Andrea
Subject: FW: TIME SENSITIVE - Memo to DM - Privacy Commissioner Visit April 14, 2011
Importance: High

Darlene,

Comments from NS Ops. MM

From: MacDonald, Michael
Sent: April 12, 2011 12:44 PM
To: Brock, Darlene; Galadza, Larisa; Davies, John
Cc: Nixon, Jennifer; Coburn, Stacey; Moshonas, Jennifer; Kwavnick, Andrea; Hawrylak, Maciek; Chayer, Marie-Helene
Subject: RE: TIME SENSITIVE - Memo to DM - Privacy Commissioner Visit April 14, 2011
Importance: High

Hi Darlene,

We don't use RDIMS. Can you please send us the actual memo in Word, and we will add some material related to the first comment.

Thanks M

From: Brock, Darlene
Sent: April 12, 2011 10:59 AM
To: Galadza, Larisa; MacDonald, Michael
Cc: Nixon, Jennifer; Coburn, Stacey
Subject: TIME SENSITIVE - Memo to DM - Privacy Commissioner Visit April 14, 2011
Importance: High

Michael/Larisa - the Privacy Commissioner is coming in to meet with Ex Comm on Thursday and in preparation for that mtg we had drafted a background note for the DM (RDIMS 406086). In reviewing the first draft, Paul had a number of comments given his time in EMNS and suggested I follow up with the two of to supplement the note. I have given you full access to the document so you can provide supplemental access to staff in your area if required. Following are Paul's specific comments on the memo and relevant section cut out of the memo (full copy attached for context)

COMMENT: Provide EMNS perspective - there have been many meetings with OPC & seems like we could say more for DM (in ref to bullet below re lawful access)

25/11/2011

000072

- The Privacy Commissioner has been critical of the Government's lawful access initiative. The issue was raised in her 2009-10 annual report to Parliament, and, more recently, on March 9, 2011, Commissioner Stoddart, along with all provincial and territorial privacy guardians, sent a letter to you regarding the privacy risks stemming from the proposed amendments to the lawful access initiative, particularly Bill C-52, the *Investigating and Preventing Criminal Electronic Communications Act*. This letter outlined the privacy concerns about the absence of limits on access powers, the wide scope of information required to be collected and provided by telecommunications companies without a warrant, and the inadequacy of internal controls and the legislative gaps in the oversight model. EMNS is in the process of drafting a response to this letter.

COMMENT: This we need to give DM something on how we are preparing from this audit - don't want to get the question without some sense of the answer (with respect to Passenger Protect)

- In November 2009, the Office of the Privacy Commissioner published a report on the Audit of the Passenger Protect Program at Transport Canada. The Audit report noted that Transport Canada had made changes to comply with recommendations dealing with information provided to the DM and with the department's oversight role of airlines under the program; and that commitments were also made to undertake activities to improve its practices for the enhancement and protection of Canadians' sensitive personnel information; and review and adjust its existing Certification and Accreditation processes based on best practices and guidelines. The OPC noted that they would conduct a follow-up to this audit exercise in two years to verify progress made in implementing responses to their recommendations. Now that Public Safety has taken over part of this program, the Commissioner may make mention of some of the concerns she had as a result of that audit and what, if anything, the Department may be doing to follow-up on the recommendations.

If possible, would like to get new version up to Paul by COB today. Thanks in advance for your assistance in this regard.

Darlene
Darlene Brock
Director, Executive Services/Directrice, Services exécutifs
Strategic Policy/Politique stratégique
Public Safety Canada/Sécurité publique Canada
269 Laurier Avenue West/269, avenue Laurier Ouest
Ottawa, Ontario K1A 0P8
Telephone/Téléphone : (613) 949-4330
Email/Courriel : Darlene.Brock@ps-sp.gc.ca

Hawrylak, Maciek

From: Kwavnick, Andrea
Sent: April 13, 2011 8:46 AM
To: Hawrylak, Maciek
Subject: FW: TIME SENSITIVE - Memo to DM - Privacy Commissioner Visit April 14, 2011
Importance: High
Attachments: PS-SP-#406086-v2-Memo_to_DM_-_Privacy_Commissioner_Visit_April_14__2011 - NSOD
Comments_V2.DOC

From: MacDonald, Michael
Sent: April 12, 2011 4:52 PM
To: Brock, Darlene
Cc: Coburn, Stacey; Moshonas, Jennifer; Chayer, Marie-Helene; Kwavnick, Andrea
Subject: FW: TIME SENSITIVE - Memo to DM - Privacy Commissioner Visit April 14, 2011
Importance: High

Darlene,

Comments from NS Ops. MM

From: MacDonald, Michael
Sent: April 12, 2011 12:44 PM
To: Brock, Darlene; Galadza, Larisa; Davies, John
Cc: Nixon, Jennifer; Coburn, Stacey; Moshonas, Jennifer; Kwavnick, Andrea; Hawrylak, Maciek; Chayer, Marie-Helene
Subject: RE: TIME SENSITIVE - Memo to DM - Privacy Commissioner Visit April 14, 2011
Importance: High

Hi Darlene,

We don't use RDIMS. Can you please send us the actual memo in Word, and we will add some material related to the first comment.

Thanks M

From: Brock, Darlene
Sent: April 12, 2011 10:59 AM
To: Galadza, Larisa; MacDonald, Michael
Cc: Nixon, Jennifer; Coburn, Stacey
Subject: TIME SENSITIVE - Memo to DM - Privacy Commissioner Visit April 14, 2011
Importance: High

Michael/Larisa - the Privacy Commissioner is coming in to meet with Ex Comm on Thursday and in preparation for that mtg we had drafted a background note for the DM (RDIMS 406086). In reviewing the first draft, Paul had a number of comments given his time in EMNS and suggested I follow up with the two of to supplement the note. I have given you full access to the document so you can provide supplemental access to staff in your area if required. Following are Paul's specific comments on the memo and relevant section cut out of the memo (full copy attached for context)

000074

24/11/2011

COMMENT: Provide EMNS perspective - there have been many meetings with OPC & seems like we could say more for DM (in ref to bullet below re lawful access)

- The Privacy Commissioner has been critical of the Government's lawful access initiative. The issue was raised in her 2009-10 annual report to Parliament, and, more recently, on March 9, 2011, Commissioner Stoddart, along with all provincial and territorial privacy guardians, sent a letter to you regarding the privacy risks stemming from the proposed amendments to the lawful access initiative, particularly Bill C-52, the *Investigating and Preventing Criminal Electronic Communications Act*. This letter outlined the privacy concerns about the absence of limits on access powers, the wide scope of information required to be collected and provided by telecommunications companies without a warrant, and the inadequacy of internal controls and the legislative gaps in the oversight model. EMNS is in the process of drafting a response to this letter.

COMMENT: This we need to give DM something on how we are preparing from this audit - don't want to get the question without some sense of the answer (with respect to Passenger Protect)

- In November 2009, the Office of the Privacy Commissioner published a report on the Audit of the Passenger Protect Program at Transport Canada. The Audit report noted that Transport Canada had made changes to comply with recommendations dealing with information provided to the DM and with the department's oversight role of airlines under the program; and that commitments were also made to undertake activities to improve its practices for the enhancement and protection of Canadians' sensitive personnel information; and review and adjust its existing Certification and Accreditation processes based on best practices and guidelines. The OPC noted that they would conduct a follow-up to this audit exercise in two years to verify progress made in implementing responses to their recommendations. Now that Public Safety has taken over part of this program, the Commissioner may make mention of some of the concerns she had as a result of that audit and what, if anything, the Department may be doing to follow-up on the recommendations.

If possible, would like to get new version up to Paul by COB today. Thanks in advance for your assistance in this regard.

Darlene
Darlene Brock
Director, Executive Services/Directrice, Services exécutifs
Strategic Policy/Politique stratégique
Public Safety Canada/Sécurité publique Canada
269 Laurier Avenue West/269, avenue Laurier Ouest
Ottawa, Ontario K1A 0P8
Telephone/Téléphone : (613) 949-4330
Email/Courriel : Darlene.Brock@ps-sp.gc.ca

**Pages 76 to / à 79
are not relevant
sont non pertinentes**

Scott, Marcie

From: Moshonas, Jennifer
Sent: April 14, 2011 11:37 AM
To: Chayer, Marie-Helene
Subject: While you were away - TIME SENSITIVE - Memo to DM - Privacy Commissioner Visit April 14, 2011
Importance: High
Attachments: PS-SP-#406086-v2-Memo_to_DM_-_Privacy_Commissioner_Visit_April_14__2011 - NSOD Comments_V2.DOC

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: MacDonald, Michael
Sent: April 12, 2011 4:52 PM
To: Brock, Darlene
Cc: Coburn, Stacey; Moshonas, Jennifer; Chayer, Marie-Helene; Kwavnick, Andrea
Subject: FW: TIME SENSITIVE - Memo to DM - Privacy Commissioner Visit April 14, 2011
Importance: High

Darlene,

Comments from NS Ops. MM

From: MacDonald, Michael
Sent: April 12, 2011 12:44 PM
To: Brock, Darlene; Galadza, Larisa; Davies, John
Cc: Nixon, Jennifer; Coburn, Stacey; Moshonas, Jennifer; Kwavnick, Andrea; Hawrylak, Maciek; Chayer, Marie-Helene
Subject: RE: TIME SENSITIVE - Memo to DM - Privacy Commissioner Visit April 14, 2011
Importance: High

Hi Darlene,

We don't use RDIMS. Can you please send us the actual memo in Word, and we will add some material related to the first comment.

Thanks M

From: Brock, Darlene
Sent: April 12, 2011 10:59 AM

000080

25/11/2011

To: Galadza, Larisa; MacDonald, Michael
Cc: Nixon, Jennifer; Coburn, Stacey
Subject: TIME SENSITIVE - Memo to DM - Privacy Commissioner Visit April 14, 2011
Importance: High

Michael/Larisa - the Privacy Commissioner is coming in to meet with Ex Comm on Thursday and in preparation for that mtg we had drafted a background note for the DM (RDIMS 406086). In reviewing the first draft, Paul had a number of comments given his time in EMNS and suggested I follow up with the two of to supplement the note. I have given you full access to the document so you can provide supplemental access to staff in your area if required. Following are Paul's specific comments on the memo and relevant section cut out of the memo (full copy attached for context)

COMMENT: Provide EMNS perspective - there have been many meetings with OPC & seems like we could say more for DM (in ref to bullet below re lawful access)

- o The Privacy Commissioner has been critical of the Government's lawful access initiative. The issue was raised in her 2009-10 annual report to Parliament, and, more recently, on March 9, 2011, Commissioner Stoddart, along with all provincial and territorial privacy guardians, sent a letter to you regarding the privacy risks stemming from the proposed amendments to the lawful access initiative, particularly Bill C-52, the *Investigating and Preventing Criminal Electronic Communications Act*. This letter outlined the privacy concerns about the absence of limits on access powers, the wide scope of information required to be collected and provided by telecommunications companies without a warrant, and the inadequacy of internal controls and the legislative gaps in the oversight model. EMNS is in the process of drafting a response to this letter.

COMMENT: This we need to give DM something on how we are preparing from this audit - don't want to get the question without some sense of the answer (with respect to Passenger Protect)

- o In November 2009, the Office of the Privacy Commissioner published a report on the Audit of the Passenger Protect Program at Transport Canada. The Audit report noted that Transport Canada had made changes to comply with recommendations dealing with information provided to the DM and with the department's oversight role of airlines under the program; and that commitments were also made to undertake activities to improve its practices for the enhancement and protection of Canadians' sensitive personnel information; and review and adjust its existing Certification and Accreditation processes based on best practices and guidelines. The OPC noted that they would conduct a follow-up to this audit exercise in two years to verify progress made in implementing responses to their recommendations. Now that Public Safety has taken over part of this program, the Commissioner may make mention of some of the concerns she had as a result of that audit and what, if anything, the Department may be doing to follow-up on the recommendations.

If possible, would like to get new version up to Paul by COB today. Thanks in advance for your assistance in this regard.

Darlene
Darlene Brock
Director, Executive Services/Directrice, Services exécutifs
Strategic Policy/Politique stratégique
Public Safety Canada/Sécurité publique Canada
269 Laurier Avenue West/269, avenue Laurier Ouest
Ottawa, Ontario K1A 0P8
Telephone/Téléphone : (613) 949-4330
Email/Courriel : Darlene.Brock@ps-sp.gc.ca

000081

25/11/2011

**Pages 82 to / à 85
are not relevant
sont non pertinentes**

**Pages 86 to / à 89
are not relevant
sont non pertinentes**

Scott, Marcie

From: Coburn, Stacey
Sent: April 20, 2011 11:20 AM
To: Chayer, Marie-Helene
Cc: Wong, Suki
Subject: URGENT TASKING: Ministerial Transition Book - Input on Key Domestic Partners/Stakeholders
Importance: High

Hi – on the consolidated transition note that deals with engagement with key domestic partners and stakeholders, the ADM SPB has requested some additional info on lawful access. However, after discussing with intergovernmental affairs (Ron Fortin) his recommendation was that we might want to take the reference out altogether since: 1. this document focuses more on stakeholders such as the Red Cross, Cdn Electricity Association, that sort of thing; and 2. We flag privacy issues and the Privacy Commissioners' concerns in our Major Policy Issues deck, indicating that officials will continue to explore options to further protect the privacy rights of Canadians.

Please advise if you agree to remove the reference to LA /Privacy Commissioner engagement from this note.

For context – our initial input can be found below, along with the question from the ADM SPB:

Paragraph provided by NS:

Provincial and Federal Privacy Commissioners have expressed concern with aspects of the subscriber information provisions of proposed lawful access legislation. Consultations with the Office of the Privacy Commissioner have informed the development of the privacy safeguards in various legislative proposals. Continued dialogue with privacy advocates would ensure the right balance of measures that would support law enforcement and national security organizations in their operations, while respecting the privacy rights of Canadians.

Privacy Advocates:

- **Through what mechanisms and how frequently does the dialogue between the Minister of Public Safety and privacy advocates, i.e. provincial privacy commissioners, occur?**

000090

25/11/2011

**Pages 91 to / à 93
are not relevant
sont non pertinentes**

Scott, Marcie

From: Audcent, Karen [kaudcent@justice.gc.ca]
Sent: May 11, 2011 10:06 AM
To: Kwavnick, Andrea; Kousha, Hasti; Dincoy, Rana; Gordon KIRK; Alter, Susan (RCMP); Bernard.Tremblay@rcmp-grc.gc.ca; mark.flynn@rcmp-grc.gc.ca; Chayer, Marie-Helene; Scrivens, Mark
Subject: FW: Blog entries on Lawful Access - Macleans.ca & Michael Geist

FYI

> -----
> From: Media-Relations-Medias
> Sent: 2011-May-11 9:50 AM
> To: Audcent, Karen; Angers, Lucie; Sansom, Gareth; * CB - Regions/ Régions; * PLS Directors; Abramchuk, Barbara; Aubie, Michael; Basran, Bill; Bernardo, Andrew; Beveridge, Tom; Bindman, Stephen; Bolton, Kathy; Breton, Genevieve; Bron, Karen; Brown, Catharine; Butcher, Joan; Chapman, Brenda; Collin, Pierre; Côté, Yves; Couto, Francisco; Davie, Katherine; Davis, Darrin; d'Eon, Pamela; Dunn, John; Ermuth, Pamela; Fakirani, Salim; Fothergill, Simon; Fulton, Megan; Gagnon, Meagan; Gaudreau, Lyne; Girouard, Christian; Goldstone, Jennifer; Gowing, Andrew; Hassan, Sandra; Hjartarson, Lynn; Keyes, John Mark; Kim, Natasha; Kirvan, Myles; Kobernick, Carolyn; Kratchanov, Denis; Laforce, Valerie; Legault, Pierre; Lyon, Carla; McCurry, Pam; McKinnon, Catherine; McLeod, Ian W (FCY); Miller, Janice; Oliver, Joel; Piragoff, Donald; Rose, Hugh; Saindon, Carole; Savard, Angela; Saville, Suesan; Schnob, Daniel; Shenher, Paul; Stephens, Pamela; Stewart, Glenda; Sugunasiri, Shalin; Therrien, Daniel; Van Loon, Christina; Van-Erum, Micheline; Vlemmiks, Danielle; Ward, Eric; Wright, Laurie
> Subject: Blog entries on Lawful Access - Macleans.ca & Michael Geist
>
>
> Blogs:
> 1. Will anonymity and hyperlinks be illegal in Canada? - Jesse Brown,
> Macleans.ca 2. The Lawful Access Legislation: Does it Really
> Criminalize Linking & Anonymity? - Michael Geist
>
> *****
>
> 1.
>
> Will anonymity and hyperlinks be illegal in Canada?
> by Jesse Brown on Tuesday, May 10, 2011 5:20pm
>
> <http://www2.macleans.ca/2011/05/10/will-anonymity-and-hyperlinks-be-illegal-in-canada/>
>
> I> '> ve blogged before about Stephen Harper> '> s tough-guy campaign promise to bundle up and ram through a bunch of crime bills within 100 days of gaining his majority. One of the three bills he> '> s mashing together deals with online crime, focusing of course on the usual boogeymen: child porn and hate speech. I> '> ve pointed to one atrocious aspect therein> -> Lawful Access, which will allow police to demand all sorts of information about Canadians from their ISPs without having to bother with pesky warrants.
>
> Here are two more reasons to be very concerned about/appalled with the upcoming legislation:
>
> It can make linking illegal.
>
> From the Library of Parliament> '> s legislative summary:
>
> Clause 5 of the bill provides that the offences of public incitement of hatred and wilful promotion of hatred may be committed> ...> by creating a hyperlink that directs web surfers to a website where hate material is posted.
>
> That> '> s just stunningly ignorant. Let> '> s put aside the ridiculous leap of reason

that equates linking to something with saying something, and instead direct our attention to the sheer stupidity of this law on technological grounds. Namely, we usually do not have control of the things we link to. They can change. So if something I link to later becomes > "> hate material> "> then I will suddenly be guilty of a hate crime. Any sound legal advice in a country where such a law exists would be to stop using hyperlinks entirely, as they present too great a liability. And that would sort of kind of make the Internet itself illegal.

>
> It can make anonymity and pseudonyms illegal.

>
> Here> '> s the Library of Parliament explaining a change from an earlier version of the bill:

>
> > ...> regarding the offences of sending a message in a false name (via) telegram, radio and telephone. Clause 11 of the bill amends those offences by removing the references to those specific communication technologies and, for some of those offences, substituting a reference to any means of telecommunication. As a result, it will be possible to lay charges in respect of those offences regardless of the transmission method or technology used.

>
> Wow. No > "> false names> "> on the Internet (or through telegrams, which bothers me less). Real names only kids> -> that> '> ll thwart the perverts!

>
> To be clear: I do not believe that the Harper government is plotting to criminalize the Internet itself. Hey, Lawful Access started as Liberal legislaion! But whoever wrote it, it> '> s a terrible and stupid piece of law, and one that would never have survived committee in one piece. But Stephen Harper has promised to ram this stuff through, and now he has the majority to do it.

>
> Shouldn> '> t someone tell him what> '> s in there?

>
> *****
> 2.

>
> The Lawful Access Legislation: Does it Really Criminalize Linking & Anonymity?
> Michael Geist
> <http://www.michaelgeist.ca/content/view/5794/125/>
> Wednesday May 11, 2011

>
> The government's plans to include lawful access provisions within its omnibus crime bill has attracted mounting attention in recent days as many commentators express concern that the legislation could create criminal liability for linking to content that incites hatred and for using anonymous or false names online. The concerns started at the Free Dominion site and have since spread to Brian Lilley at the Toronto Sun and Jesse Brown's blog at Maclean's.

>
> As I have argued for a long time, there are many reasons to be concerned with lawful access. The government has never provided adequate evidence on the need for it, it has never been subject to committee review, it would mandate disclosure of some personal information without court oversight, it would establish a massive ISP regulatory process (including employee background checks), it would install broad new surveillance technologies, and it would cost millions (without a sense of who actually pays). Given these problems, it is not surprising to find that every privacy commissioner in Canada has signed a joint letter expressing their concerns.

>
> Yet while lawful access raises many issues (such that it clearly does not belong in an omnibus bill placed on the fast track), I do not believe that creating criminal liability for linking or anonymous speech are among them.

>
> The source of the latest round of concern stems from the Library of Parliament's Parliamentary Information and Research Service legislative summary of Bill C-51. On the issue of hyperlinking, it states:

>
> Clause 5 of the bill provides that the offences of public incitement of hatred and wilful promotion of hatred may be committed by any means of communication and include making hate material available, by creating a hyperlink that directs web surfers to a

website where hate material is posted, for example.

>
> I must admit that I think is wrong. The actual legislative change amends the definition of communicating from this:

>
> "> communicating> "> includes communicating by telephone,
> broadcasting or other audible or visible means;

>
> to this:

>
> "> communicating> "> means communicating by any means and includes
> making available;

>
> The revised definition is obviously designed to broaden the scope of the public incitement of hatred provision by making it technology neutral. Whereas the current provision is potentially limited to certain technologies, the new provision would cover any form of communication. It does not specifically reference hyperlinking.

>
> I recognize that one could make an argument that a link could be included within communicating by any means or making available, but that strikes me a big stretch. The Supreme Court of Canada is examining this issue within the context of libel in the Crookes v. Newton case which should provide further guidance on the meaning of a "link" under Canadian law. In the earlier B.C. Court of Appeal decision, a majority of the court concluded that merely linking to another site does not make that person a publisher of the material found at that site. Pending the outcome of that case, I think the legislative summary likely overstates the breadth of the provision. >

>
> I similarly think the anonymity concerns are overstated. The legislative summary on this issue states:

>
> The existing provisions of the Code regarding the offences of sending a message in a false name and sending false information, indecent remarks or > "> harassing> "> messages (the French term > "> harassants> "> currently used in subsection 372(3) of the Code is replaced by > "> harcelants> "> in the bill) refer to certain communication technologies used to commit those offences, such as telegram, radio and telephone. Clause 11 of the bill amends those offences by removing the references to those specific communication technologies and, for some of those offences, substituting a reference to any means of telecommunication. As a result, it will be possible to lay charges in respect of those offences regardless of the transmission method or technology used.

>
> This summary had led to concerns that this prohibits false names on the Internet. The problem with the summary is that it doesn't mention that the provision includes an "intent to injure or alarm" component. The full provision states:

>
> Everyone commits an offence who, with intent to injure or alarm a person, conveys information that they know is false, or causes such information to be conveyed by letter or any means of telecommunication.

>
> In other words, the offence is not conveying false information, but rather conveying false information with the intent to injure or alarm. This does not stop people from posting anonymously, unless they do so with the intent to injure or alarm, in which case arguably they should not be shielded from liability merely because they are using the Internet.

>
> While I am skeptical about the interpretation involving linking and anonymity liability, the latest round of concerns provide a textbook illustration of why the lawful access bills should not be included in the omnibus crime legislation. Lawful access is complex legislation that touches on a very wide range of issues, many of which extend far beyond conventional criminal law. They are not part of the group of bills that advanced through the legislative process but ultimately stalled. Given that the proposals breed uncertainty and have never been the subject of committee hearings or debate, lumping them together with many other bills represents a serious threat and is bound to result in only a cursory review of an important piece of legislation.

>

>
>
>

Scott, Marcie

From: Kwavnick, Andrea
Sent: May 12, 2011 4:03 PM
To: Chayer, Marie-Helene
Subject: Additional Information

Marie,

Below is additional information for the Support section:

Similarly, while consultations with Privacy Commissioners have informed the development of privacy safeguards included in the proposed legislation, Provincial and Federal Privacy Commissioners have expressed concern with the subscriber information provisions of the proposed legislation, in particular the requirement for service providers to release this basic information without a warrant. As well, some representatives of Canada's telecommunications industry have, during previous consultations, expressed concern regarding the cost of implementing the obligations of the proposed legislation. In order to alleviate these concerns, the proposed legislation is flexible and contains a number of mechanisms to minimize the cost to service providers.

Thanks
Andrea

25/11/2011

000098

Page 99
is not relevant
est non pertinente

Hawrylak, Maciek

From: Paulson, Erika
Sent: May 17, 2011 9:46 AM
To: Kwavnick, Andrea; Hawrylak, Maciek
Subject: RE: Heads up - media request - Georgia Straight

Issues Mg't will take the approved MLs and propose a response to you, which you can tweak/recommend changes to/do a signals check on in your shop. The text at the bottom of my FYI is all the info we have from the reporter's email.

Erika Paulson
Tel: 613-993-4415

-----Original Message-----

From: Kwavnick, Andrea
Sent: May 17, 2011 9:42 AM
To: Paulson, Erika; Hawrylak, Maciek
Subject: Re: Heads up - media request - Georgia Straight

Hi Erika,

Will comms be drafting a response and sending it to us for review or are we to draft the response?

Also, is the email below all we have from the reporter, or is there a more formal letter or request?

Thanks
Andrea

----- Original Message -----

From: Paulson, Erika
To: Kwavnick, Andrea; Hawrylak, Maciek
Sent: Tue May 17 09:37:43 2011
Subject: RE: Heads up - media request - Georgia Straight

Hey Andrea - got your msg RE timelines for this. My issues mg't team will lay out their desired deadlines, but as long as it's delivered before 8pm tonight (per journo's 5pm PST deadline), it should be fine. Since the response will be based heavily on pre-approved messaging, hopefully it'll be a relatively painless process.

If you have any more questions, please feel free to give me a shout. Maybe I'll see you at the Town Hall!

Cheers,
Erika Paulson
Tel: 613-993-4415

-----Original Message-----

From: Paulson, Erika
Sent: May 17, 2011 8:45 AM
To: Kwavnick, Andrea; Hawrylak, Maciek
Subject: Heads up - media request - Georgia Straight

FYI - My Issues Management team received the following media request last night from the Georgia Straight. They'll work w you this morning on a response, based on the attached doc I sent you in a while ago in prep for the letter from the priv commiss.

Cheers
Erika

Date: 16 May 2011

Reporter: The Georgia Straight, @STRAIGHT.COM
Issue: Reporter is requesting interview with a ministry official or spokesperson who can

address issues raised by Canada's privacy commissioners on 'lawful access' proposals.
Reference can be found at: http://www.priv.gc.ca/media/nr-c/2011/let_110309_e.cfm
(letter to DM from Privacy Commissioner, March 9, 2011).

Deadline: Tuesday, May 17, 5 p.m. (PST)
Action: Consulting policy

**Pages 102 to / à 104
are duplicates of
sont des duplicatas des
pages 32 to / à 34**

Kwavnick, Andrea

From: Chayer, Marie-Helene
Sent: May 18, 2011 9:07 AM
To: Fergusson, Janis
Cc: Burton, Meredith; Kwavnick, Andrea; MacDonald, Michael
Subject: RE: For review and approval - media request - Lawful Access
Janis,

Here is what we would say:

"Public Safety and Justice officials have been discussing lawful access legislation with Privacy Commissioners for many years. Their comments and advice have informed legislative proposals and will continue to contribute to this important initiative."

Thanks

MH

From: Fergusson, Janis
Sent: May 18, 2011 8:45 AM
To: Chayer, Marie-Helene
Cc: Burton, Meredith; Paulson, Erika; Kwavnick, Andrea; MacDonald, Michael
Subject: RE: For review and approval - media request - Lawful Access

ok sounds good

From: Chayer, Marie-Helene
Sent: May 18, 2011 8:42 AM
To: Fergusson, Janis
Cc: Burton, Meredith; Paulson, Erika; Kwavnick, Andrea; MacDonald, Michael
Subject: RE: For review and approval - media request - Lawful Access

I'm not sure we want to go that far. Let me think about it for a minute - I'll send you shortly.

From: Fergusson, Janis
Sent: May 18, 2011 8:40 AM
To: Chayer, Marie-Helene
Cc: Burton, Meredith; Paulson, Erika; Kwavnick, Andrea; MacDonald, Michael
Subject: RE: For review and approval - media request - Lawful Access

The changes look fine from this end.

Would it be ok to add this as a last bullet as a way to respond to the open letter to the DM?:

We continue to work with privacy commissioners and take their advice into consideration.

From: Chayer, Marie-Helene

000105

24/11/2011

RE: For review and approval - media request - Lawful Access

Sent: May 18, 2011 8:37 AM
To: Fergusson, Janis
Cc: Burton, Meredith; Paulson, Erika; Kwavnick, Andrea; MacDonald, Michael
Subject: FW: For review and approval - media request - Lawful Access

Good morning,

We reviewed the lines you sent last night and would request that you make these small changes (see below new text in red.)

Please call me if you have any questions.

Thanks

Marie-Hélène

From: Fergusson, Janis
To: MacDonald, Michael; Davies, John; Mungall, Richard
Cc: Burton, Meredith; Paulson, Erika; Filipps, Lisa; McDonald, Jessica
Sent: Tue May 17 19:49:47 2011
Subject: FW: For review and approval - media request - Lawful Access

Hello,

We made some slight adjustments to the media lines. Could you review and advise if you have any concerns?
The reporter has agreed to an extension of tomorrow morning.

Thanks,

Janis

- o The Government of Canada is committed to the safety and security of Canadians and their communities.

- o The former Bill C-52, the *Investigating and Preventing Criminal Electronic Communications Act*, was created to help keep Canadians safe from those who would use communications technology to pursue criminal or terrorist activities.

- o The Act, which died on the Order Paper with the Federal election, contained two main elements:
 - The first element was a requirement that telecommunications service providers develop and maintain the technical capability to allow for the lawful interception of ~~technology required to lawfully intercept~~ communications. This would ensure that the police and CSIS would be able to implement a warrant to intercept an individual's communications.

 - The legislation would not have provided new powers to intercept communications. The existing warrant processes for the interception of private communications would not have changed.

 - The second element was a requirement for service providers to provide, upon request, basic subscriber information to specifically designated police, CSIS and Competition Bureau officials to support their investigations and, during emergencies, to provide this information to any requesting police officer.

24/11/2011

000106

- Subscriber information refers to the basic information about a customer that is held by a telecommunications service provider and includes a subscriber's name, address, telephone number, email and Internet Protocol address and certain cellular identifiers.

- It does not include a history of websites visited, the content of emails or information pertaining to phone calls a person made or received. Accessing such information will continue to require a warrant.

- The legislation was drafted to provide for a balanced and well-regulated administrative regime for the disclosure of basic subscriber information, and also included a number of privacy safeguards developed as a result of consultations with Privacy Commissioners:

- Authorities would have been required to conduct regular audits on the practices and procedures with respect to accessing basic subscriber information; and

1 The number of designated officials who could have requested this information would have been limited to either 5 employees or 5% of an organization's work force, whichever was greater.

- Many other countries, including the United Kingdom, the United States, Australia, Germany and Sweden, already have similar laws in place to ensure intercept capability and access to basic subscriber information for their respective law enforcement and national security agencies.

From: Chayer, Marie-Helene
Sent: May 17, 2011 1:39 PM
To: Fergusson, Janis
Cc: Burton, Meredith; Paulson, Erika; Kwavnick, Andrea
Subject: RE: For review and approval - media request - Lawful Access

Janis,

Here is what we suggest. It was approved by our DG.

Please let me know if you have any questions/concerns.

Thanks

Marie-Hélène

- The Government of Canada is committed to the safety and security of Canadians and their communities.
- Former Bill C-52, the *Investigating and Preventing Criminal Electronic Communications Act*, was created to help keep Canadians safe from those who would use communications technology to pursue criminal or terrorist activities.
- The Act, which died on the Order Paper with the Federal election, contained two main elements. The first

element was a requirement that telecommunications service providers develop and maintain a technical capability to allow for the lawful interception of communications. This would ensure that the police and CSIS – once they have received judicial authorization to intercept an individual's communications – would be able to technically implement that authorization.

- The legislation would not have provided new powers to intercept communications. The existing authorization processes for the interception of private communications would not have changed.
- The second element was a requirement for service providers to provide, upon request, basic subscriber information to specifically designated police, CSIS and Competition Bureau officials in support of their investigative duties. This information was also to have been made available during exceptional and urgent circumstances to any requesting police officers.
- Subscriber information refers to the basic information about a customer that is held by a telecommunications service provider and includes a subscriber's name, address, telephone number, email and Internet Protocol address and certain cellular identifiers. It does not include a history of websites visited, the content of emails or information pertaining to phone calls a person made or received. Accessing such information will continue to require a judicially authorized warrant.
- The legislation was drafted to provide for a balanced and well-regulated administrative regime for the disclosure of basic subscriber information, and also included a number of privacy safeguards developed as a result of consultations with Privacy Commissioners. For example, authorities would have been required to conduct regular audits on the practices and procedures with respect to accessing basic subscriber information. As well, the number of designated officials who could have requested this information would have been limited to either 5 employees or 5% of an organization's work force, whichever was greater.
- Of note, under the *Personal Information Protection and Electronic Documents Act*, service providers are already allowed to provide basic subscriber information to law enforcement and national security agencies on a voluntary basis, but are not compelled to do so.
- Many other countries, including the United Kingdom, the United States, Australia, Germany and Sweden, already have similar laws in place to ensure intercept capability and access to basic subscriber information for their respective law enforcement and national security agencies.

From: Fergusson, Janis

Sent: May 17, 2011 11:54 AM

To: Hawrylak, Maciek; Kwavnick, Andrea; MacDonald, Michael; Chayer, Marie-Helene

Cc: Burton, Meredith; Paulson, Erika; Filippis, Lisa; McDonald, Jessica

Subject: RE: For review and approval - media request - Lawful Access

Importance: High

Further to this request, the Minister's Office said it would be helpful if the answer noted that Section 16 of the legislation would not permit the RCMP to obtain someone's history of websites visited – or anything else -without a court approved warrant. Do we have existing messages that allude to that? We will need

to move proposed messaging up to the MO soon. Thanks in advance for your assistance.

Janis

From: Fergusson, Janis
Sent: May 17, 2011 9:46 AM
To: Hawrylak, Maciek; Kwavnick, Andrea; MacDonald, Michael; Chayer, Marie-Helene
Cc: Burton, Meredith; Paulson, Erika; Filippis, Lisa; McDonald, Jessica
Subject: For review and approval - media request - Lawful Access

Hello,

We received a media request last night on lawful access. We recommend declining the interview request however we would offer a written response. Below are the most recent high-level approved media lines. Could you have a look and advise if you have any concerns/edits?

Thanks,

Janis Fergusson
Media Relations
949-4288

Date: 16 May 2011

Reporter: The Georgia Straight, @STRAIGHT.COM

Issue: Reporter is requesting interview with a ministry official or spokesperson who can address issues raised by Canada's privacy commissioners on 'lawful access' proposals. Reference can be found at: http://www.priv.gc.ca/media/nr-c/2011/let_110309_e.cfm (letter to DM from Privacy Commissioner, March 9, 2011).

Deadline: Tuesday, May 17, 5 p.m. (PST)

Action: Consulting policy

MEDIA LINES:

- The Government of Canada is committed to the safety and security of Canadians and their communities.
- This legislation was drafted to help keep Canadians safe from those who would use new communications technology to pursue criminal or terrorist activities.
- The *Investigating and Preventing Criminal Electronic Communications Act* was drafted to ensure that

law enforcement and CSIS can keep pace with new communication technologies and are able to execute judicially authorized warrants.

- The legislation drafted did not provide new powers to intercept communications. The warrant processes for the interception of private communications would not change with this Bill.
- The legislation was drafted to provide for a balanced and well-regulated administrative regime for the disclosure of basic subscriber information to the police, CSIS and the Competition Bureau when requested.
- Canada drafted this bill to join many other countries including the United Kingdom, the United States, Australia, Germany and Sweden, which already have similar laws to ensure intercept capability and the sharing of basic subscriber information.

<< File: PS-SP-#398703-v2-MLs_-_Lawful_Access_-_tenses_changed_during_election.DOC >>

**Pages 111 to / à 112
are duplicates of
sont des duplicatas des
pages 114 to / à 115**

MacDonald, Michael

From: MacDonald, Michael
Sent: May-18-11 4:23 PM
To: Chayer, Marie-Helene
Subject: Re: TASKING: Lawful Access

Agreed. Th

From: Chayer, Marie-Helene
To: MacDonald, Michael
Cc: Haeck, Kimberly; Johnston, Shannon
Sent: Wed May 18 16:00:06 2011
Subject: RE: TASKING: Lawful Access

Mike,

I just spoke to Chantal and asked her to talk to comms. We were of course aware of the article, which was in fact a re-print from a TS article published over the weekend, and were not surprised by its content.

If MO wants to respond (and I'm not sure it would be advisable at this point), it could be done through a letter to the editor – which would be developed by comms with our assistance.

Chantal will connect with comms and let us know what is required from us, if anything.

I'll keep you posted,

MH

From: Johnston, Shannon
Sent: May 18, 2011 3:50 PM
To: Chayer, Marie-Helene
Cc: Haeck, Kimberly; MacDonald, Michael
Subject: TASKING: Lawful Access
Importance: High

Marie-Hélène,

The introduction of an omnibus crime bill (an article which appeared in the Ottawa Citizen) will likely include legislation creating new surveillance requirements and police powers (nicknamed "lawful access"). The article criticizes the absence of extensive debate in the House of Commons and has never been the subject of committee hearing. It also raises privacy and free speech concerns.

<http://www.ottawacitizen.com/Tories+heighten+surveillance+powers/4794162/story.html>

The Minister's Office is asking for clarification as to whether the Department is aware of this article; if there is any action being taken to respond to the article; has the Department consulted with the Department of Justice, given that the legislation also falls under the mandate of the Department of Justice, etc.

Could you please prepare a memorandum to the Minister on this issue.

****Note the memorandum should also include a response to the MO's question in the e-mail below.**

Please prepare memo to DGO by **4:00om May 19** as Mike will be away on Friday, May 20.

Thank you

Shannon Johnston
National Security Operations / Opérations de la sécurité nationale
949-4623

From: Dupuis, Chantal
Sent: Wednesday, May 18, 2011 3:44 PM
To: MacDonald, Michael
Cc: Johnston, Shannon; Haeck, Kimberly; Coburn, Stacey; Piasko, Ruba; Dupuis, Chantal
Subject: TASKING: Lawful Access

(For action)

Good afternoon,

An article appeared in the Ottawa Citizen (see link below) regarding the introduction of an omnibus crime bill and that it will likely include legislation creating new surveillance requirements and police powers (nicknamed "lawful access"). The article criticizes the absence of extensive debate in the House of Commons and has never been the subject of committee hearing. It also raises privacy and free speech concerns.

<http://www.ottawacitizen.com/Tories+heighten+surveillance+powers/4794162/story.html>

The Minister's Office is asking for clarification as to whether the Department is aware of this article; if there is any action being taken to respond to the article; has the Department consulted with the Department of Justice, given that the legislation also falls under the mandate of the Department of Justice, etc.

Could you please prepare a memorandum to the Minister on this issue.

Please note the memorandum should also include a response to the MO's question in the e-mail below.

Please prepare memo signed/approved and return to ADMO via Ruba Piasko by **16:00 May 24**.

merci

Chantal Dupuis

Policy Coordinator / Coordinatrice de politiques
Office of the Assistant Deputy Minister / Bureau du Sous-ministre adjointe
Emergency Management and National Security Branch / Secteur de la Gestion des mesures d'urgence et de la Sécurité nationale
Public Safety Canada / Sécurité publique Canada

Tel: 613-990-9270

This is an extract from the Privacy Commissioner's letter to the DM regarding this bill

Respective roles of the federal, provincial and territorial privacy offices

From our perspective, in relation to oversight, perhaps even more problematic is clause 20(6) which creates an obligation for the federal Office of the Privacy Commissioner to "report on the powers that they [public officers] have to conduct audits similar to those referred to in subject clause 20(4) with respect to police services constituted under the laws of their province." While the OPC has jurisdiction over the Royal Canadian Mounted Police, this provision does not adequately address the issue of those municipal or provincial police services that are not subject to the jurisdiction of a provincial or territorial privacy office or the OPC.

Nor does the Bill resolve the legislative gap in jurisdictions where privacy officers do not have the powers necessary to audit compliance by provincial and municipal police forces. These gaps are evident in many jurisdictions. While recognizing that the federal Office of the Privacy Commissioner could exercise its audit provisions over the RCMP, this issue still strikes the provincial and territorial commissioners as a significant concern at the local level. Certainly it raises risks for privacy and diminishes the value of meaningful, timely review.

The concern that there is no oversight of the municipal or provincial police services accessing information under this legislation may be legitimate. Could you ask the department to provide an analysis of this issue ASAP?

Scott, Marcie

From: Burton, Meredith
Sent: May 19, 2011 9:16 AM
To: Chayer, Marie-Helene
Cc: Filippis, Lisa
Subject: RE: Response to recent Ottawa Citizen article
Attachments: 2009_09_11_Op_ed_approved - FR.doc; 2009-09-11_Op ed_approved_rev.doc

Hi Marie-Helene. I was out of the office yesterday afternoon, so am just now following up on the letter to the editor angle. I understand the MO was wondering if you/the department recommends a letter to the editor. Please let me know if you have made a recommendation.

In the meantime, I'm attaching an OP-Ed we prepared some time ago in response to criticisms (unfounded) by the privacy commissioners.

If you decide to move forward on the letter to the editor, we should ensure the media relations team are looped in. I've cc'ed their manager Lisa Filippis for her awareness.

Cheers, Meredith

From: Hawrylak, Maciek
Sent: Wednesday, May 18, 2011 5:08 PM
To: Burton, Meredith
Cc: Chayer, Marie-Helene
Subject: Response to recent Ottawa Citizen article

Meredith,

Marie-Helene has tasked me with preparing a memo for the Minister regarding the recent Ottawa Citizen article on lawful access. I understand Marie left you a voicemail to this effect.

Just to keep you in the loop, we are preparing our response for tomorrow morning, in which we'll identify certain inaccuracies but recommend against responding directly, given that there is no lawful access legislation currently before Parliament. We will suggest that if the legislation is reintroduced, comms material addressing these issues raised in the Citizen article will be assembled and disseminated.

If you have any questions, please let me know.

Regards,
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

Op-Ed – Bill C-47

I would like to respond to some remarks made by the Federal, Provincial and Territorial Privacy Commissioners. While I have great respect for the work they do, I feel there have been some misunderstandings about Bill C-47, the Technical Assistance to Law Enforcement in the 21st Century Act. As such, I believe clarification is needed.

First, let's start with what Bill C-47 is not: It is not about intercepting or eavesdropping on the private communications of Canadians. Nor is it about monitoring the web surfing habits of Canadians or preventing them from sending anonymous e-mails.

The proposals in Bill C-47 are about ensuring that law enforcement can keep up with new communication technologies and continue to implement warrants authorized by the courts. New technology is a powerful tool however, in the hands of criminals and terrorists, this technology can be used in ways that threaten public safety. The Government of Canada needs to update Canadian laws to keep pace with new technology – a step already taken by many of our international partners.

I want to be clear: The legislation provides no new powers to intercept communications. The existing requirements for judicial authorization for intercepts will be maintained. Since 1974, police in Canada have been authorized to intercept private communications when a court order is issued by a judge who believes on reasonable grounds that a serious offence, such as child pornography, drug trafficking, money laundering or murder, has been or will be committed. The judge must also be satisfied that authorizing the intercept is in the best interests of the administration of justice and that other investigative procedures have been tried and failed.

Nothing proposed in Bill C-47 will change these limits. Nor will it upset the strong balance established between the protection of privacy, human rights and the safety of our citizens, which are values we all cherish.

Today, telephone and Internet companies are not required to build intercept capabilities into their networks. Because of this, even with a court order, police may not be able to intercept communications. Under Bill C-47, communications providers would be required to update their systems to enable interceptions approved by the courts. To avoid undue burden, the proposed law would allow companies to build this capability gradually over time.

There have also been misunderstandings about the Government's proposals for police and CSIS to obtain subscriber information. Basic subscriber information such as a customer's name, address, telephone number and Internet address can be valuable at the initial stages of an investigation.

The problem is that while some service providers give subscriber information to law enforcement upon request, others fail to provide it in a timely fashion, or refuse to provide it at all. This has created a difference in industry practices across the country.

Access to subscriber information is particularly important in the online context, as criminals use the internet to operate with anonymity. For example, in cases where a child is lured over the internet by a sexual predator, often the only clue police have as to the identity of the perpetrator is an IP address associated with a chat room. In these situations, police need to quickly establish the identity of the suspect based on the IP address. In several cases, service providers have refused to share this information, thereby leaving some children at risk. This proposed legislation will help to ensure that there are no more dead-end investigations.

The proposed legislation would require telephone and internet companies to provide this information to designated law enforcement and CSIS officials without a warrant. Bill C-47 includes some of the very safeguards identified by the privacy commissioners to protect privacy, such as the requirement to track who is requesting the information and why, to permit audit and oversight of how the information is handled, and a five year Parliamentary review.

Canadians can rest assured that any updates to our legislative regime will respect the privacy and human rights entrenched in laws

such as the *Canadian Charter of Rights and Freedoms*, the *Privacy Act*, and the *Personal Information Protection and Electronic Documents Act*.

Lettre d'opinion – Projet de loi C-47

Je souhaite, par la présente, répondre à des commentaires émis par les commissaires à la protection de la vie privée du Canada, des provinces et des territoires. Bien que j'aie beaucoup de respect pour le travail qu'ils font et que je partage leurs préoccupations au sujet des droits à la vie privée des Canadiens, j'ai l'impression qu'ils ont mal compris le projet de loi C-47, la *Loi sur l'assistance au contrôle d'application des lois au 21^e siècle*. En conséquence, je crois qu'une clarification s'impose.

D'abord, commençons par ce que le projet de loi C-47 n'est pas : son intention n'est pas de permettre l'interception ou l'écoute des communications privées des Canadiens ni de surveiller leurs habitudes de navigation sur le Web ni de les empêcher d'envoyer des courriels sous le couvert de l'anonymat.

Les propositions incluses dans le projet de loi C-47 visent à donner aux organismes d'application de la loi la possibilité de s'adapter aux nouvelles technologies de communication et de continuer à exécuter les mandats émis par les tribunaux. La nouvelle technologie est un outil puissant; cependant, entre les mains des criminels et des terroristes, elle pourrait être utilisée pour menacer la sécurité publique. Le gouvernement du Canada doit moderniser ses lois afin de s'adapter à la nouvelle technologie – mesure déjà prise par un grand nombre de nos partenaires internationaux.

Je veux être très net : Le projet de loi ne donne pas de nouveaux pouvoirs pour l'interception des communications. Les exigences actuelles visant les autorisations judiciaires relatives aux interceptions seront maintenues. Depuis 1974 au Canada, la police peut intercepter des communications privées à la suite d'un mandat émis par un juge, qui a des motifs raisonnables de croire qu'une infraction grave, telle que la pornographie juvénile, le trafic de drogues, le blanchiment d'argent ou un meurtre, a été ou sera commise. Le juge doit aussi être convaincu que l'autorisation d'interception est dans l'intérêt de l'administration de la justice et que d'autres méthodes d'enquête se sont soldées par un échec.

Aucune des propositions incluses dans le projet de loi C-47 ne changera ces limites et ne viendra non plus perturber le solide équilibre maintenu entre la protection de la vie privée, les droits de la personne et la sécurité de nos citoyens, des valeurs qui nous sont chères.

À l'heure actuelle, les compagnies de téléphone et d'Internet ne sont pas obligées d'intégrer à leurs réseaux les moyens d'interception. Alors, même munie d'un mandat, la police n'est pas toujours en mesure d'intercepter les communications. En vertu du projet de loi C-47, les télécommunicateurs seront tenus d'actualiser leurs systèmes afin de permettre les interceptions autorisées par les tribunaux. Pour qu'elles ne soient pas écrasées par un lourd fardeau, les compagnies pourront, en vertu du projet de loi, échelonner sur une période de temps l'ajout progressif de ces moyens.

Il y a également eu des malentendus au sujet des propositions du gouvernement visant l'obtention par la police ou le Service canadien du renseignement de sécurité (SCRS) de renseignements sur les abonnés. Des renseignements de base sur les abonnés, comme les noms, adresse, numéro de téléphone et adresse de courriel, peuvent s'avérer utiles au tout début d'une enquête.

Des fournisseurs de services donnent sur demande aux agents d'application de la loi les renseignements sur les abonnés. L'ennui est que d'autres refusent de le faire ou, s'ils le font, ne donnent pas l'information en temps utile. Cette situation a créé des disparités au pays pour ce qui est des pratiques de l'industrie.

L'accès aux renseignements sur les abonnés est particulièrement important dans l'environnement virtuel, étant donné que les criminels se servent d'Internet pour agir sous le couvert de l'anonymat. Par exemple, dans les cas d'enfants qui sont la proie de prédateurs sexuels qui opèrent sur Internet, souvent l'adresse IP d'un salon de clavardage est l'unique indice que possèdent les policiers sur l'identité des contrevenants. Dans ce genre de situation, la police devrait pouvoir identifier rapidement les suspects d'après l'adresse IP. Il est arrivé à plusieurs reprises que des fournisseurs de services refusent de communiquer l'information, laissant ainsi des enfants dans des situations dangereuses. Les propositions législatives

aideront à faire en sorte qu'il n'y ait plus d'enquêtes qui tournent court.

En vertu du projet de loi, les entreprises de téléphone et d'Internet sont tenues de fournir les renseignements aux agents d'application de la loi ou du SCRS, même sans mandat. Le projet de loi C-47 renferme certains des mêmes dispositifs de protection mentionnés par les commissaires à la protection de la vie privée, tels que l'obligation de surveiller le demandeur des renseignements et de vérifier le motif de la demande, l'autorisation de vérifier et de surveiller la manière dont les renseignements sont utilisés et la tenue d'un examen quinquennal par le Parlement.

Les Canadiens n'ont pas de craintes à avoir; toutes modifications à notre régime législatif respecteront les droits de la personne et de protection des renseignements personnels qui sont garantis par des lois telles que la *Charte canadienne des droits et libertés*, la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques*.

Hawrylak, Maciek

From: Paulson, Erika
Sent: May 19, 2011 2:13 PM
To: Chayer, Marie-Helene; Kwavnick, Andrea; Hawrylak, Maciek; Dincoy, Rana
Cc: Burton, Meredith; Fergusson, Janis
Subject: FYI - Federal "lawful access" bills concern B.C. privacy commissioner
Importance: Low

FYI - article from the Georgia Straight request for MLs. Although Janis delivered our response well before the reporter's deadline, it was not integrated in the article.

Erika

EXCERPT (full article below):

These will give the police, the Canadian Security Intelligence Service, and the Competition Bureau greater powers to intercept online communications and gather information about Internet users. The legislation will also allow law-enforcement authorities to remotely activate tracking devices found in mobile phones and GPS devices in cars.

"What's at stake is surveillance of their personal information, particularly their access to the Internet, without their knowledge and without judicial oversight," Denham said about the potential impact of these measures on citizens' rights.

...

On March 9, Denham and other privacy commissioners across the country wrote to deputy public safety minister William Baker to express their reservations about the snooping bills.

According to Denham, Baker has acknowledged their letter and stated that he is looking into their concerns.

Federal "lawful access" bills concern B.C. privacy commissioner

By Carlito Pablo, May 19, 2011

B.C.'s information and privacy commissioner says Canadians should be worried about the anticipated reintroduction of federal legislation that will give police and government spies broader powers to snoop on citizens.

"That turns our whole system of rights on its head, because we have the right of personal privacy,"

000123

24/11/2011

Elizabeth Denham told the *Straight* in a phone interview. "We have the right to free speech, and it's the government that has to make the case when they intrude upon these rights."

Denham was referring to bills C-50, C-51, and C-52, which died on the order paper when the Conservative government of Prime Minister **Stephen Harper** was defeated on March 25, triggering a federal election.

With a majority mandate, the Harper government is expected to introduce and approve a bundle of anticrime-related legislation within its first 100 days in office, including proposals that will enhance the state's capacity to spy on its own citizens without a court warrant.

These will give the police, the Canadian Security Intelligence Service, and the Competition Bureau greater powers to intercept online communications and gather information about Internet users. The legislation will also allow law-enforcement authorities to remotely activate tracking devices found in mobile phones and GPS devices in cars.

"What's at stake is surveillance of their personal information, particularly their access to the Internet, without their knowledge and without judicial oversight," Denham said about the potential impact of these measures on citizens' rights.

Previous federal Liberal governments have also tried to introduce such measures, and groups like the B.C. Freedom of Information and Privacy Association have opposed these "lawful access" bills.

"We traditionally depend on the police having to go through certain steps before they can breach our privacy, the argument being privacy is an important part of the rights of citizens in a democratic society," B.C. FIPA president **Richard Rosenberg** told the *Straight* by phone.

The bills will provide the government unrestricted access to subscriber information held by Internet service providers and telecommunications companies. SFU assistant communications professor **Peter Chow-White** finds this disconcerting.

"Internet providers are not under any obligation to give up personal information to law enforcement without due process," Chow-White told the *Straight* by phone. "This reduces that due process."

On March 9, Denham and other privacy commissioners across the country wrote to deputy public safety minister **William Baker** to express their reservations about the snooping bills.

According to Denham, Baker has acknowledged their letter and stated that he is looking into their concerns.

<http://www.straight.com/article-393297/vancouver/federal-bills-concern-bc-privacy-commish>

Erika Paulson
Senior Communications Advisor | Conseillère principale en communications
Communications - Emergency Management and National Security | Sécurité nationale et gestion des urgences
- Communications
Public Safety Canada | Sécurité publique Canada
Tel: 613-993-4415
Fax: 613-993-7062
Erika.Paulson@ps-sp.gc.ca

Scott, Marcie

From: Hawrylak, Maciek
Sent: May 26, 2011 1:07 PM
To: Chayer, Marie-Helene
Subject: RE: TASKING: Lawful Access

Marie,

I've given Kim the folder back to give to you when you're available. I couldn't condense the whole thing down to 2 pages while also hitting even briefly on each of the points you jotted down in pencil, so we're at 3 pages. You'll also note that I addressed the provincial privacy commissioner issue with subsection 20 (6), as requested by Chantal Dupuis below and confirmed with her by phone.

I have not updated the disk as I presume you'll have additional changes.

I'll be here all afternoon to make changes.

Maciek

From: Chayer, Marie-Helene
Sent: May 18, 2011 4:11 PM
To: Hawrylak, Maciek
Subject: FW: TASKING: Lawful Access
Importance: High

From: Johnston, Shannon
Sent: May 18, 2011 3:50 PM
To: Chayer, Marie-Helene
Cc: Haeck, Kimberly; MacDonald, Michael
Subject: TASKING: Lawful Access
Importance: High

Marie-Hélène,

The introduction of an omnibus crime bill (an article which appeared in the Ottawa Citizen) will likely include legislation creating new surveillance requirements and police powers (nicknamed "lawful access"). The article criticizes the absence of extensive debate in the House of Commons and has never been the subject of committee hearing. It also raises privacy and free speech concerns.

<http://www.ottawacitizen.com/Tories+heighten+surveillance+powers/4794162/story.html>

The Minister's Office is asking for clarification as to whether the Department is aware of this article; if there is any action being taken to respond to the article; has the Department consulted with the Department of Justice, given that the legislation also falls under the mandate of the Department of Justice, etc.

Could you please prepare a memorandum to the Minister on this issue.

**Note the memorandum should also include a response to the MO's question in the e-mail below.

25/11/2011

000125

Page 4 of 5

Please prepare memo to DGO by **4:00om May 19** as Mike will be away on Friday, May 20.

Thank you

Shannon Johnston
National Security Operations / Opérations de la sécurité nationale
949-4623

From: Dupuis, Chantal
Sent: Wednesday, May 18, 2011 3:44 PM
To: MacDonald, Michael
Cc: Johnston, Shannon; Haeck, Kimberly; Coburn, Stacey; Piasko, Ruba; Dupuis, Chantal
Subject: TASKING: Lawful Access

(For action)

Good afternoon,

An article appeared in the Ottawa Citizen (see link below) regarding the introduction of an omnibus crime bill and that it will likely include legislation creating new surveillance requirements and police powers (nicknamed "lawful access"). The article criticizes the absence of extensive debate in the House of Commons and has never been the subject of committee hearing. It also raises privacy and free speech concerns.

<http://www.ottawacitizen.com/Tories+heighten+surveillance+powers/4794162/story.html>

The Minister's Office is asking for clarification as to whether the Department is aware of this article; if there is any action being taken to respond to the article; has the Department consulted with the Department of Justice, given that the legislation also falls under the mandate of the Department of Justice, etc.

Could you please prepare a memorandum to the Minister on this issue.

Please note the memorandum should also include a response to the MO's question in the e-mail below.

Please prepare memo signed/approved and return to ADMO via Ruba Piasko by **16:00 May 24**.

merci

Chantal Dupuis

Policy Coordinator / Coordinatrice de politiques
Office of the Assistant Deputy Minister / Bureau du Sous-ministre adjointe
Emergency Management and National Security Branch / Secteur de la Gestion des mesures d'urgence et de la Sécurité nationale
Public Safety Canada / Sécurité publique Canada

Tel: 613-990-9270

This is an extract from the Privacy Commissioner's letter to the DM regarding this bill

Respective roles of the federal, provincial and territorial privacy offices

From our perspective, in relation to oversight, perhaps even more problematic is clause 20(6) which creates an obligation for the federal Office of the Privacy Commissioner to "report on the powers that they [public officers] have to conduct audits similar to those referred to in subject clause 20(4) with respect to police services constituted under the laws of their province." While the OPC has jurisdiction over the Royal Canadian Mounted Police, this provision does not adequately address the issue of those municipal or provincial police services that are not subject to the jurisdiction of a provincial or territorial privacy office or the OPC.

Nor does the Bill resolve the legislative gap in jurisdictions where privacy officers do not have the powers necessary to audit compliance by provincial and municipal police forces. These gaps are evident in many jurisdictions. While recognizing that the federal Office of the Privacy Commissioner could exercise its audit provisions over the RCMP, this

issue still strikes the provincial and territorial commissioners as a significant concern at the local level. Certainly it raises risks for privacy and diminishes the value of meaningful, timely review.

The concern that there is no oversight of the municipal or provincial police services accessing information under this legislation may be legitimate. Could you ask the department to provide an analysis of this issue ASAP?

MacDonald, Michael

From: MacDonald, Michael
Sent: June-09-11 1:19 PM
To: Chayer, Marie-Helene
Subject: Re: Speakers' Series -- Privacy, Surveillance, and Public Safety // Série de conférences -- Protection de la vie privée, surveillance et sécurité publique

Sounds good. M

From: Chayer, Marie-Helene
To: MacDonald, Michael
Sent: Thu Jun 09 13:14:27 2011
Subject: Fw: Speakers' Series -- Privacy, Surveillance, and Public Safety // Série de conférences -- Protection de la vie privée, surveillance et sécurité publique

Mike,

Fyi - Rana will attend the Privacy Commissioner's speakers' series on June 23rd.

Mh

From: Dincoy, Rana
To: Chayer, Marie-Helene
Sent: Thu Jun 09 10:23:37 2011
Subject: RE: Speakers' Series -- Privacy, Surveillance, and Public Safety // Série de conférences -- Protection de la vie privée, surveillance et sécurité publique

OK. My RSVP has been accepted.

Rana Dincoy
Senior Policy Analyst – Investigative Technology and Telecommunications Policy /
Analyste principale en politiques – Politique sur les technologies d'enquêtes et les télécommunications
National Security Operations Division / Division des Opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
(613)991-3240

From: Chayer, Marie-Helene
Sent: June 9, 2011 8:18 AM
To: Dincoy, Rana
Subject: RE: Speakers' Series -- Privacy, Surveillance, and Public Safety // Série de conférences -- Protection de la vie privée, surveillance et sécurité publique

Please do.

Thanks

From: Dincoy, Rana
Sent: June 7, 2011 10:04 AM
To: Chayer, Marie-Helene; Kwavnick, Andrea; Hawrylak, Maciek; Thompson, Julie
Subject: RE: Speakers' Series -- Privacy, Surveillance, and Public Safety // Série de conférences -- Protection de la vie privée, surveillance et sécurité publique

Yes I think so, and I'd be happy to go.

Rana Dincoy
Senior Policy Analyst – Investigative Technology and Telecommunications Policy /
Analyste principale en politiques – Politique sur les technologies d'enquêtes et les télécommunications
National Security Operations Division / Division des Opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
(613)991-3240

From: Chayer, Marie-Helene
Sent: June 7, 2011 7:44 AM
To: Kwavnick, Andrea; Dincoy, Rana; Hawrylak, Maciek; Thompson, Julie
Subject: FW: Speakers' Series -- Privacy, Surveillance, and Public Safety // Série de conférences -- Protection de la vie privée, surveillance et sécurité publique

Good morning,

Do you think it would make sense for one of us to attend?

Marie

From: Burton, Meredith
Sent: June 6, 2011 10:32 AM
To: Van Criekingen, Jane; Paulson, Erika; Chayer, Marie-Helene
Subject: RE: Speakers' Series -- Privacy, Surveillance, and Public Safety // Série de conférences -- Protection de la vie privée, surveillance et sécurité publique

Very interesting. I think we should have someone there. Thanks Jane!

Erika, and Marie-Helene, fyi.

From: Van Criekingen, Jane
Sent: Monday, June 06, 2011 10:24 AM
To: Burton, Meredith
Subject: FW: Speakers' Series -- Privacy, Surveillance, and Public Safety // Série de conférences -- Protection de la vie privée, surveillance et sécurité publique

Hi Meredith,

A colleague of mine, who works at the Office of the Privacy Commissioner of Canada, passed along this email for a learning event that they are hosting. Since it relates to privacy, surveillance, issues of National Security and Public Safety, I thought I'd pass it along to you. Feel free to pass along to your team or any of your policy folks that might be interested in attending.

Cheers,

Jane Van Criekingen
Strategist, Social Media | Stratège, médias sociaux
Communication Services | Services de Communication
Public Safety Canada | Sécurité publique Canada
Jane.VanCriekingen@ps-sp.gc.ca
Tel: (613) 949-4488

From: Erin Courtland [mailto:Erin.Courtland@priv.gc.ca]
Sent: June 3, 2011 9:42 AM

To: Van Crieking, Jane

Subject: Speakers' Series -- Privacy, Surveillance, and Public Safety // Série de conférences -- Protection de la vie privée, surveillance et sécurité publique

La version française suit.

Speakers' Series – Privacy, Surveillance, and Public Safety

On June 23rd, 2011, our Office is holding the fourth *Insights on Privacy* armchair discussion. We heard in April about opportunities for privacy in the design of intimate devices that we share our lives with every day, like smart phones, and the sensor-rich landscape that's upon us.

To complement this talk, we've invited [David Murakami Wood](#) and [Craig Forcese](#) to examine the privacy risks in a society that is placing its citizens under greater surveillance with each passing year.

David Murakami Wood is an Associate Professor in the Department of Sociology at [Queen's University](#) and holds a Canada Research Chair (Tier 2) in Surveillance Studies. Until August 2009, he was Reader in Surveillance Studies in the *Global Urban Research Unit* at *Newcastle University* in the UK. He had an ESRC Research Fellowship for a project called *Cultures of Urban Surveillance*, which looked at the globalization of surveillance in different global cities. David is a member of *The Surveillance Studies Centre* at Queen's and is part of *The New Transparency* research initiative. He is also Managing Editor of *Surveillance & Society*, the international journal of surveillance studies, and a founder-member of the *Surveillance Studies Network*.

Craig Forcese, LL.M, has been an Associate Professor in the Faculty of Law at the [University of Ottawa](#) since 2003. Previously, he practiced international trade law with Hughes Hubbard & Reed LLP in Washington D.C., representing clients in proceedings before the *U.S. Department of Commerce*, the *U.S. International Trade Commission*, the *U.S. Trade Representative*, and the *World Trade Organization*. He also served as a law clerk for Mr. Justice Andrew MacKay at the *Federal Court of Canada*. Craig is the author of a number of books on law and national security, and a frequent blogger.

To participate:

We are inviting full participation in this discussion. For those of you who attend the session in person, we will be asking for questions from the audience as well as inviting you to tweet the content using the #privtalks hashtag.

If you are unable to attend the session in person, and would like the speakers to address a particular aspect of this topic, please send your question to knowledge.savoir@priv.gc.ca by June 20th and we will try to incorporate it in the issues we cover.

The video of this event will be made available after the presentation, as we've done for [previous Speakers Series events](#).

Space is limited and is available on a first-come, first-served basis. Please RSVP before June 20, 2011. Simultaneous interpretation for both official languages will be available.

When: 2:00-4:00 p.m. Thursday, June 23, 2011

Where: Minto Suites Hotel, 185 Lyon Street North, 2nd Floor, Salon Vanier/Stanley

RSVP: knowledge.savoir@priv.gc.ca

Série de conférences — Protection de la vie privée, surveillance et sécurité publique

La quatrième discussion informelle dans le cadre de la série de conférences « Le point sur la vie privée » du Commissariat à la protection de la vie privée se tiendra le 23 juin 2011. Nous avons discuté, lors de la séance du mois d'avril, de la possibilité de prendre en compte les principes de protection de la vie privée à même la conception des

appareils personnels, tels les téléphones intelligents, avec lesquels nous partageons notre quotidien, et dans un environnement où prolifèrent de multiples capteurs.

Pour poursuivre la discussion, nous avons demandé à [David Murakami Wood](#) et à [Craig Forcese](#) d'examiner les risques liés à la protection de la vie privée dans une société qui soumet ses citoyens à une surveillance de plus en plus étroite chaque année.

David Murakami Wood est professeur agrégé au Département de sociologie de l'[Université Queen's](#) depuis août 2009 et est titulaire d'une chaire de recherche du Canada sur la surveillance. Avant son arrivée à Queen's, il avait été chargé de cours dans le domaine de la surveillance à l'Unité de la recherche urbaine globale de l'Université de Newcastle au Royaume-Uni. Récipiendiaire d'une bourse de recherche postdoctorale de l'ESRC pour un projet intitulé « Cultures of Urban Surveillance » (Cultures de la surveillance urbaine), il s'est intéressé à la mondialisation de la surveillance dans des grandes villes à rayonnement mondial. David est membre du Centre des études sur la surveillance de l'Université Queen's et participe au projet de recherche ayant pour titre « New Transparency » (Une nouvelle transparence). Il est également rédacteur en chef de *Surveillance & Society*, la revue internationale des études sur la surveillance, et membre fondateur du Réseau des études sur la surveillance.

Craig Forcese est professeur agrégé à la Faculté de droit de l'[Université d'Ottawa](#) depuis 2003. Auparavant, il a pratiqué le droit du commerce international dans le cabinet Hughes Hubbard et Reed LLP à Washington (D.C.). Ses fonctions consistaient à représenter des clients dans des litiges devant le département du Commerce américain, la Commission américaine du commerce international, le représentant américain au Commerce et l'Organisation mondiale du commerce. Il a également été l'adjoint du juge Andrew MacKay à la Cour fédérale du Canada. Enfin, Craig a écrit de nombreux ouvrages sur le droit et la sécurité nationale, en plus d'être un blogueur assidu.

Pour participer :

Nous vous invitons à participer en grand nombre à cette discussion. Ceux d'entre vous qui assisteront à la séance en personne seront invités à poser des questions et à diffuser le contenu des échanges à l'aide de Twitter (#privtalks hashtag).

Si vous ne pouvez être sur place, mais aimeriez que les présentateurs abordent un sujet en particulier, veuillez nous faire parvenir votre question à knowledge.savoir@priv.gc.ca avant le 20 juin et nous tenterons de l'ajouter à la liste de sujets.

L'enregistrement vidéo de cette conférence sera disponible après la présentation, comme cela a été le cas pour les [séances précédentes](#).

Le nombre de places étant limité, celles-ci sont offertes selon le principe du premier arrivé, premier servi. Veuillez confirmer votre présence avant le 20 juin 2011. Des services d'interprétation simultanée seront disponibles dans les deux langues officielles.

Quand : De 14 h à 16 h, le jeudi 23 juin 2011

Où : Hôtel Minto Suites, 185, rue Lyon Nord, 2^e étage, Salon Vanier/Stansley

Veuillez confirmer votre présence à l'adresse suivante : knowledge.savoir@priv.gc.ca

Erin Courtland

Research Analyst | Analyste de la recherche

Legal Services, Policy and Research Branch | Direction des services juridiques – politiques et recherche

Office of the Privacy Commissioner of Canada | Commissariat à la protection de la vie privée du Canada

112 Kent St, 2nd Floor

Ottawa, ON K1A 1H3

☎ (613) 947-8423

Cell:

erin.courtland@priv.gc.ca

Confidentiality Notice: This e-mail message (including attachments, if any) is intended for the use of the individual or entity to which it is addressed and may contain information that is privileged, proprietary, confidential and exempt from disclosure. If you are not the intended recipient, you are notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify the sender and erase this e-mail message immediately.

Avis de confidentialité : Le présent message électronique (y compris les pièces qui y sont annexées, le cas échéant) s'adresse au destinataire indiqué et peut contenir des renseignements de caractère privé ou confidentiel. Si vous n'êtes pas le destinataire de ce document, nous vous signalons qu'il est strictement interdit de le diffuser, de le distribuer ou de le reproduire. Si ce message vous a été transmis par erreur, veuillez en informer l'expéditeur et le supprimer immédiatement.

MacDonald, Michael

From: Coburn, Stacey
Sent: June-13-11 4:48 PM
To: MacDonald, Michael
Cc: Kwavnick, Andrea; Moshonas, Jennifer
Subject: RE: para

Great – thanks!

Stacey Coburn
949-4490

From: MacDonald, Michael
Sent: Monday, June 13, 2011 4:39 PM
To: Coburn, Stacey
Cc: Kwavnick, Andrea; Moshonas, Jennifer
Subject: RE: para
Importance: High

Looks good – we like it

From: Coburn, Stacey
Sent: June 13, 2011 4:15 PM
To: MacDonald, Michael
Subject: para

Further, at the request of provincial privacy commissioners (in order to draw attention to potential gaps in their ability to audit provincial and municipal law enforcement agencies' use of the provisions in the proposed legislation), former Bill C-52 contained a provision that would have required the federal Privacy Commissioner to report to Parliament on the auditing powers of provincial privacy commissioners.

Stacey Coburn
Special Advisor | Conseillère spéciale
Office of the Assistant Deputy Minister | Cabinet de la Sous-ministre adjointe
Emergency Management and National Security | Gestion des mesures d'urgence et de la sécurité nationale
Public Safety Canada | Sécurité publique Canada
Tel/Tél: 613-949-4490 | Fax/Télec: 613-990-8301
www.publicsafety.gc.ca | www.securitepublique.gc.ca

COPY



Public Safety / Sécurité publique
Canada / Canada

Deputy Minister / Sous-ministre

Ottawa, Canada
K1A 0P8

JUN 16 2011

UNCLASSIFIED

DATE:

File No.: 6950-1 / 379965
RDIMS No.: 425577

MEMORANDUM FOR THE MINISTER

**PRIVACY CONSIDERATIONS:
LAWFUL ACCESS LEGISLATION**

(Information only)

ISSUE

In response to a request from your office, this memorandum provides information regarding the potential privacy impacts of the former Bill C-52, the *Investigating and Preventing Criminal Electronic Communications Act*, particularly as they relate to concerns raised by privacy commissioners and the media.

BACKGROUND

In anticipation of the potential reintroduction in Parliament of former lawful access related bills, the federal Privacy Commissioner and her provincial counterparts (**TAB A**), as well as Dr. Michael Geist, law professor at the University of Ottawa (**TAB B**), recently raised concerns with the privacy impacts specifically related to the former Bill C-52.

Former Bill C-52 consisted of two key components with respect to telecommunications service providers (TSPs): first, that they develop and maintain intercept capable systems; and second, that they provide basic subscriber information to authorities upon request. While some TSPs already have at least partially intercept capable systems and provide subscriber information on request, others do not, which significantly impedes investigations.

Departmental officials have met with privacy stakeholders on numerous occasions to discuss various iterations of this legislation. On December 15, 2010, I met with the federal Privacy Commissioner, Jennifer Stoddard, to address some of her concerns and outline the safeguards built into former Bill C-52. Despite extensive consultations, privacy advocates remain critical of the legislation.

.../2

UNCLASSIFIED

In their letters and articles, the privacy advocates maintain that the Government has not clearly demonstrated the need for lawful access legislation. The majority of the privacy concerns focus on the requirement for TSPs to provide basic subscriber information (e.g. name, address, phone number and cellular phone identifiers) to designated police, Canadian Security Intelligence Service (CSIS) and Competition Bureau officials upon request. Specifically, privacy advocates have argued that:

- authorities' power to request subscriber information should be limited and subject to judicial authorization;
- the proposed legislation contained insufficient oversight mechanisms; and
- the auditing provisions set out in the proposed legislation were not clear.

CONSIDERATIONS

Officials have demonstrated the operational need for lawful access legislation on multiple occasions, including during broad public consultations in 2002, 2005, 2007, and, more recently, when legislation was introduced in Parliament in 2009, and 2010.

Presently, TSPs cannot and do not comply with judicially authorized interception warrants if they do not have the technical capability to do so. Former Bill C-52 would have ensured that TSPs build and maintain the technical capability to intercept communications. The proposed legislation, however, would not have changed existing laws governing the interception of communications. As such, law enforcement and national security agencies would have continued to require a warrant for the interception of communications.

Basic subscriber information is often required at the earliest stages of an investigation in order to secure a warrant for other investigative techniques, such as interception. Requiring a warrant to access basic subscriber information would contravene existing practice under the *Personal Information Protection and Electronic Documents Act* (PIPEDA), through which TSPs may already voluntarily release subscriber information to authorities. Former Bill C-52 would have simply regularized what is an *ad hoc* process under PIPEDA by compelling TSPs to provide this information upon request.

Recognizing that providing authorities with access to basic subscriber information is a sensitive topic for many Canadians, former Bill C-52 included a series of strong privacy safeguards. For example, only designated officials from law enforcement and intelligence agencies could have requested such information (except during emergencies); the number of designated officials would have been limited to five percent of each organization's employees, or five employees in total, whichever number was

-3-

UNCLASSIFIED

bigger; designated officials would have had to create a record indicating the purpose of the subscriber information request; and authorities would have had to conduct regular audits on how they handle basic subscriber information requests.

Further, at the request of provincial privacy commissioners (in order to draw attention to potential gaps in their ability to audit provincial and municipal law enforcement agencies' use of the provisions in the proposed legislation), former Bill C-52 contained a provision that would have required the federal Privacy Commissioner to report to Parliament on the auditing powers of provincial privacy commissioners.

RECOMMENDATION

It is recommended that, should lawful access legislation be reintroduced in Parliament, the privacy safeguards of the legislation continue to be highlighted in all communications materials.

Should you require additional information, please do not hesitate to contact me or Lynda Clairmont, Assistant Deputy Minister, Emergency Management and National Security, at 613-990-4976.

Original Signed by
William V. Baker
A Signé l'Original
William V. Baker

Enclosures: (2)

Prepared by: Maciek Hawrylak

000136



Office of the
Privacy Commissioner
of Canada

Commissionnaire
& le protecteur
de la vie privée

Office of the Privacy Commissioner of Canada

Home > Resources > Reports and Publications

Resources

- Reports and Publications
- Guidelines
- Research
- Tools and Videos
- Privacy Illustrations
- Consultations
- Privacy Impact Assessments
- Provincial/Territorial links
- International data protection authorities
- Employment Opportunities at the OPC



Reports and Publications

▶ [OPC Guidance Documents](#) ▶ [Annual Reports to Parliament](#) ▶ [Audit Reports](#) ▶ [Reports on Plans and Priorities \(RPPs\) and Departmental Performance Reports \(DPRs\)](#) ▶ [Official Languages Annual Review](#) ▶ [OPC Audits by the Office of the Auditor General and the Public Service Commission](#) ▶ [Internal Audits and Evaluation Reports](#) ▶ [Other Publications](#)

Other Publications

Letter to Public Safety Canada from Canada's Privacy Commissioners and Ombudspersons on the current 'Lawful Access' proposals

Privacy Commissioner of Canada Jennifer Stoddart, along with all provincial and territorial privacy guardians, have sent a letter to the Deputy Minister of Public Safety Canada regarding the privacy risks stemming from the government's current initiative to amend the legal regime governing the use of electronic search, seizure and surveillance. Copies of the letter, dated March 9, 2011, were also provided to members of the House of Commons Standing Committee on Public Safety and National Security, as well as the House of Commons Standing Committee on Justice and Human Rights.

March 9, 2011

Mr. William V. Baker
Deputy Minister
Public Safety Canada
269 Laurier Avenue West
Ottawa, Ontario
K1A 0P8

Dear Mr. Baker:

000137

As a group, Canada's Privacy Commissioners remain concerned about the government's current lawful access initiative, in particular Bill C-52, the *Investigating and Preventing Criminal Electronic Communications Act*. We held a teleconference on January 18, 2011 to discuss the issue and would like to relay the substance of that dialogue. While we understand the legitimate needs of law enforcement and national security agencies, as well as their challenges in the context of new information technologies, we would like to bring to your attention the following concerns about the absence of limits on the access powers, the wide scope of information required to be collected and provided by telecommunications companies without a warrant and the inadequacy of internal controls and the legislative gaps in the oversight model.

The overall lawful access initiative

Read together, the provisions of Bills C-50, C-51, and C-52 (augmented by changes in Bills C-22 and C-29) would substantially diminish the privacy rights of Canadians. They do so by enhancing the capacity of the state to conduct surveillance and access private information while reducing the frequency and vigour of judicial scrutiny. In essence, they make it easier for the state to subject more individuals to surveillance and scrutiny.

While we understand the need for law enforcement and national security agencies to function effectively in the context of new information technologies, in our view, it would be misleading to suggest that these bills will simply maintain capacity. Taken together, the proposed changes and new powers add significant new capabilities for investigators to track and search and seize digital information about individuals.

It is also noteworthy that at no time have Canadian authorities provided the public with any evidence or reasoning to suggest that CSIS or any other Canadian law enforcement agencies have been frustrated in the performance of their duties as a result of shortcomings attributable to current law, TSPs or the manner in which they operate. New powers should be demonstrably necessary as well as proportionate. Ultimately, even if Canadian authorities can show investigations are being frustrated in a digital environment, all the various powers that would be granted to address these issues must be subject to rigorous, independent oversight.

The Investigating and Preventing Criminal Electronic Communications Act (Bill C-52)

Clause 16 gives unrestricted access to subscriber data records held by telecommunications firms. We are concerned that the proposed powers are not limited in any fashion. The privacy oversight community in Canada has expressed reservations, in a joint resolution by all of Canada's privacy commissioners signed after the original tabling of similar bills in 2009. A copy of this resolution is attached.

We are concerned that clause 16 of Bill C-52 would give authorities access to a wide scope of personal information without a warrant; for example, unlisted numbers, email account data and IP addresses. The Government itself took the view that this information was sensitive enough to make trafficking in such 'identity information' a *Criminal Code* offence. Many Canadians consider this information sensitive and worthy of protection, which does not fit with the proposed self-authorized access model.

Currently, under section 487.013 of the *Criminal Code*, investigators require judicial authorization to seek client information like name, address or account numbers from a financial institution or commercial entity. As you are aware, clauses 16 and 17 of C-52 provide law enforcement, CSIS, and Competition officials with warrantless access to "subscriber information" held by telecommunications companies. In our view, law enforcement and security agency access to information linking subscribers to devices and devices to subscribers should generally be subject to prior judicial scrutiny accompanied by the appropriate checks and balances.

Lack of appropriate oversight

We are also concerned by the oversight model. Clause 20(4) sets out audit powers for the federal Office of the Privacy Commissioner (OPC) which already exists in section 18 of the *Privacy Act*. Without additional resources to the OPC, however, this additional statutory provision does not augment existing oversight.

In addition, we believe the auditing and reporting safeguards should be strengthened. In relation to internal audits required under clause 20 (2), the requirement that law enforcement and security agencies report to "the responsible minister of anything arising out of the audit that in their opinion should be brought to the attention of the minister" should be subject to an objective standard. Agencies should be expressly required to report any collection, use or retention practices that do not appear to be necessary to the duty or function for which they were originally obtained.

Respective roles of the federal, provincial and territorial privacy offices

From our perspective, in relation to oversight, perhaps even more problematic is clause 20(6) which creates an obligation for the federal Office of the Privacy Commissioner to "report on the powers that they [public officers] have to conduct audits similar to those referred to in subject clause 20(4) with respect to police services constituted under the laws of their province." While the OPC has jurisdiction over the Royal Canadian Mounted Police, this provision does not adequately address the issue of those municipal or provincial police services that are not subject to the jurisdiction of a provincial or territorial privacy office or the OPC.

Nor does the Bill resolve the legislative gap in jurisdictions where privacy officers do not have the powers necessary to audit compliance by provincial and municipal police forces. These gaps are evident in many jurisdictions. While recognizing that the federal Office of the Privacy Commissioner could exercise its audit provisions over the RCMP, this issue still strikes the provincial and territorial commissioners as a significant concern at the local level. Certainly it raises risks for privacy and diminishes the value of meaningful, timely review.

We are also concerned that very few of our organizations have been consulted in this process, particularly given the review role we are being asked to perform, flowing from clause 20 (3)(c). To this end, we would insist that the relevant federal officials reengage with provincial Offices of the Attorney-General or territorial equivalents. This should lead to a more open dialogue with the provincial commissioners on these issues.

Conclusion

We have collectively made a number of recommendations in our 2009 resolution for legislators to consider as they approach the individual pieces of legislation involved in the initiative. We believe that there is insufficient justification for the new powers, that other, less intrusive alternatives can be explored and that a focussed, tailored approach is vital. In our view, this balance has not been achieved.

To remedy these shortcomings, we suggest certain gaps need to be addressed. Provincial and territorial privacy officers would ask that the federal Privacy Commissioner, in reporting to Parliament on the adequacy of audit and investigation powers, should also be expressly authorized to report on whether privacy officers consider themselves to have adequate resources to conduct the necessary audits and reviews. As above, the federal government must commit to working with provincial and territorial governments to ensure that all of the relevant privacy officers have sufficient powers and resources.

It is our intention to provide Parliament and the public with further analysis and assistance with respect to the global privacy effect of proposed lawful access legislation. We also believe that the regulatory and reporting aspects of the initiative need to be as open and transparent as possible.

We appreciate your consideration of these concerns.

Sincerely,

Original signed by

Jennifer Stoddart,
Privacy Commissioner of Canada

signed by M. Munn (for F. Work)

Frank Work, Q.C.,
Information and Privacy Commissioner of Alberta

signed by E. Denham

Elizabeth Denham,
Information and Privacy Commissioner for British Columbia

signed by I. Hamilton

Irene Hamilton,
Ombudsman for Manitoba

signed by A. Bertrand

Anne E. Bertrand, Q.C.,
Access to Information and Privacy Commissioner of New Brunswick

signed by E. Ring

Ed Ring,
Information and Privacy Commissioner for Newfoundland and Labrador

signed by E. Keenan Bengts

Elaine Keenan Bengts,
Information and Privacy Commissioner for the Northwest Territories and
Information and Privacy Commissioner for Nunavut

signed by D. McCallum

Dulcie McCallum,
Freedom of Information and Protection of Privacy Review Officer for the Province of
Nova Scotia

signed by A. Cavoukian

Ann Cavoukian, Ph.D,
Information and Privacy Commissioner of Ontario

signed by M. MacDonald

Maria C. MacDonald,
Information and Privacy Commissioner of Prince Edward Island

signed by J. Chartier

Me Jean Chartier,
Président de la Commission d'accès à l'information du Québec

signed by R.G. Dickson

R. Gary Dickson, Q.C.,
Information and Privacy Commissioner of Saskatchewan

signed by T.A. McPhee

Tracy-Anne McPhee,
Ombudsman and Information and Privacy Commissioner of Yukon

c.c.: Chair, House of Commons Standing Committee on Justice and Human Rights
(JUST)
Chair, House of Commons Standing Committee on Public Safety and National Security
(SECU)

Encl. (1): 2009 Federal/Provincial/Territorial Resolution

Date Modified: 2011-03-24

**Pages 142 to / à 143
are duplicates of
sont des duplicatas des
pages 47 to / à 48**

Tories aim to heighten web-surveillance powers

Planned legislation threatens privacy, free speech

BY MICHAEL GEIST, CITIZEN SPECIAL MAY 17, 2011

With the new Parliamentary session scheduled to kick off within the next few weeks, two major initiatives will dominate the initial legislative agenda: passing a budget and introducing an omnibus crime bill that contains at least 11 crime-related bills. The prioritization of the crime legislation is consistent with the Conservative election platform, which included a commitment to bundle all the outstanding crime and justice bills into a single omnibus bill and to pass it within the new Parliament's first 100 days.

The Conservatives argue that the omnibus approach is needed since the opposition parties "obstructed" passage of their crime and justice reforms during successive minority governments. Yet included within the crime bill package is likely to be legislation creating new surveillance requirements and police powers that has never received extensive debate on the floor of the House of Commons and never been the subject of committee hearings.

The package is benignly nicknamed "lawful access," but isn't benign. If the Conservatives move forward with it, it would feature a three-pronged approach focused on information disclosure, mandated surveillance technologies, and new police powers.

The first prong mandates the disclosure of Internet provider customer information without court oversight. Under current privacy laws, providers may voluntarily disclose customer information but are not required to do so. The new system would require the disclosure of customer name, address, phone number, e-mail address, Internet protocol address, and a series of device identification numbers.

The second prong requires Internet providers to rework their networks to allow for real-time surveillance. The bill sets out detailed capability requirements that will eventually apply to all Canadian Internet providers. These include the power to intercept communications, to isolate the communications to a particular individual, and to engage in multiple simultaneous interceptions.

Having obtained customer information without court oversight and mandated Internet surveillance capabilities, the third prong creates several new police powers designed to obtain access to the surveillance data.

Lawful access raises genuine privacy and free speech concerns, particularly given the fact the government has never provided adequate evidence on the need for it, it has never been subject to committee review, and it would cost millions to implement yet there has been no disclosure on who would actually pay for it. Given this, it is not surprising that every privacy commissioner in Canada has signed a joint letter expressing their concerns.

Tories aim to heighten web-surveillance powers

Not only is the substance problematic, but the attempt to fast track lawful access virtually guarantees that it will not be fully vetted. For example, over the past few weeks there has been mounting concern that the legislation would also create new criminal liability for hyperlinking to content that incites hatred and for using anonymous or false names online.

The source of these concerns is a legislative summary by the Library of Parliament's Parliamentary Information and Research Service. While there is reason to doubt the interpretation involving linking and anonymity liability contained in the summary, the recent fears provide a textbook illustration of why lawful access should not be included in the omnibus crime legislation.

Lawful access is complex legislation that touches on a very wide range of issues, many of which extend far beyond conventional criminal law. Given that the proposals breed uncertainty and have never been the subject of public review, lumping them together with many other bills represents a serious threat and is bound to result in only a cursory analysis of an important piece of legislation that has far reaching consequences for privacy, security, and free speech.

Michael Geist holds the Canada Research Chair in Internet and E-commerce Law at the University of Ottawa, Faculty of Law. He can be reached at mgeist@uottawa.ca or online at www.michaelgeist.ca.

© Copyright (c) The Ottawa Citizen

MacDonald, Michael

From: bmunson@itac.ca
Sent: June-22-11 2:17 PM
To: info@itac.ca
Subject: Privacy Commissioner releases annual report, aims to make the internet a priority

ITAC Cyber Security Forum, Legal Affairs Forum and Smart Regulation Forum

The federal Privacy Commissioner table her 2010 annual report in Parliament yesterday.

<http://www.theglobeandmail.com/news/technology/tech-news/privacy-watchdog-jennifer-stoddart-makes-the-web-a-priority/article2070193/>

Here's a link to a related Globe and Mail article, titled: "Privacy watchdog Jennifer Stoddart makes the Web a priority":

<http://www.theglobeandmail.com/news/technology/tech-news/privacy-watchdog-jennifer-stoddart-makes-the-web-a-priority/article2070193/>

Bill Munson
ITAC

Drag our Leaf Icon above to your taskbar to bookmark TGAM in Internet Explorer 9.

[Show me how](#)

[Please don't show me this again](#)

[Remind me later](#)

THE GLOBE AND MAIL

Report

Privacy watchdog Jennifer Stoddart makes the Web a priority

kim mackrael

From Wednesday's Globe and Mail

Published Tuesday, Jun. 21, 2011 9:34PM EDT

Last updated Thursday, Sep. 01, 2011 7:27PM EDT

Canada's privacy watchdog is already famous for staring down Facebook and crossing swords with Google, but a new report from Jennifer Stoddart's office shows she isn't finished dealing with the two Internet giants.

"Our message to all tech titans was clear," says the Privacy Commissioner's annual report, tabled in Parliament Tuesday. "Think about privacy before you launch a new application. Don't just leave it to luck and the lawyers."

Ms. Stoddart has been in the spotlight in recent years for a public scolding of Facebook that eventually convinced the social-networking site to tighten its privacy controls. For example, Facebook acted on her recommendation to change third-party applications, which must now inform users of the kind of data they want to collect and obtain users' permission before the information is released.

Large companies are becoming more receptive to requests from privacy watchdogs to change their operations to counter possible breaches of their users' privacy, she said.

"Early on, we had a lot of trouble getting their attention," Ms. Stoddart said in an interview Tuesday.

Ms. Stoddart said she now acts in concert with other privacy regulators from around the world, adding clout to her demands that Canadians must be able to maintain control over the way their information is used and shared online.

"We are in constant dialogue with the [Office of the Privacy Commissioner], and are constantly providing them with information to address any questions or concerns they have," Victoria Freeman, a spokeswoman for Facebook, said by e-mail.

Ms. Stoddart said her office continues to investigate Facebook for other privacy concerns, including a complaint about the appearance of Facebook's "Like" buttons on other websites, but said she could not offer details about the complaint until the investigation is resolved.

Another probe into Google's Street View mapping application found the Google cars that collected images for the company's online maps also gathered private information from wireless networks in Canada. The report indicates that Google has responded to recommendations from the commissioner's office to delete or restrict access to the information and improve privacy training for Google employees.

Ms. Stoddart is concerned that companies still often have an attitude of "innovate first and let the lawyers mop up afterwards."

"I think they're doing a little bit less of that, but they're in a world that encourages them to innovate," Ms. Stoddart said, adding privacy concerns can sometimes be swept aside in a rush to beat competitors.

The report acknowledges that standards of privacy are changing as people increasingly live their lives online, but notes that most Canadians still want to be the ones in control of where their information ends up.

"Privacy remains an incredibly important and cherished value to Canadians – and to people around the world," the report states.

.....

By the numbers

207

Total number of formal complaints received in 2010

45

Number of complaints made about financial services companies, such as banks and credit intermediaries

42

Number of complaints in which personal information has been used or disclosed without meaningful consent

11

Complaints related to social networking, websites or Internet service providers

44

Private-sector data breaches that were voluntarily reported

1

Complaint that a bank disclosed a woman's personal information to her partner's ex-wife's lawyer

Compiled by Emily Jackson

© 2011 The Globe and Mail Inc. All Rights Reserved.

Drag our Leaf Icon above to your taskbar to bookmark TGAM in Internet Explorer 9.

[Show me how](#)

[Please don't show me this again](#)

[Remind me later](#)



Report

Privacy watchdog Jennifer Stoddart makes the Web a priority

kim mackrael

From Wednesday's Globe and Mail

Published Tuesday, Jun. 21, 2011 9:34PM EDT

Last updated Thursday, Sep. 01, 2011 7:27PM EDT

Canada's privacy watchdog is already famous for staring down Facebook and crossing swords with Google, but a new report from Jennifer Stoddart's office shows she isn't finished dealing with the two Internet giants.

"Our message to all tech titans was clear," says the Privacy Commissioner's annual report, tabled in Parliament Tuesday. "Think about privacy before you launch a new application. Don't just leave it to luck and the lawyers."

Ms. Stoddart has been in the spotlight in recent years for a public scolding of Facebook that eventually convinced the social-networking site to tighten its privacy controls. For example, Facebook acted on her recommendation to change third-party applications, which must now inform users of the kind of data they want to collect and obtain users' permission before the information is released.

Large companies are becoming more receptive to requests from privacy watchdogs to change their operations to counter possible breaches of their users' privacy, she said.

"Early on, we had a lot of trouble getting their attention," Ms. Stoddart said in an interview Tuesday.

Ms. Stoddart said she now acts in concert with other privacy regulators from around the world, adding clout to her demands that Canadians must be able to maintain control over the way their information is used and shared online.

"We are in constant dialogue with the [Office of the Privacy Commissioner], and are constantly providing them with information to address any questions or concerns they have," Victoria Freeman, a spokeswoman for Facebook, said by e-mail.

Ms. Stoddart said her office continues to investigate Facebook for other privacy concerns, including a complaint about the appearance of Facebook's "Like" buttons on other websites, but said she could not offer details about the complaint until the investigation is resolved.

Another probe into Google's Street View mapping application found the Google cars that collected images for the company's online maps also gathered private information from wireless networks in Canada. The report indicates that Google has responded to recommendations from the commissioner's office to delete or restrict access to the information and improve privacy training for Google employees.

Ms. Stoddart is concerned that companies still often have an attitude of "innovate first and let the lawyers mop up afterwards."

"I think they're doing a little bit less of that, but they're in a world that encourages them to innovate," Ms. Stoddart said, adding privacy concerns can sometimes be swept aside in a rush to beat competitors.

The report acknowledges that standards of privacy are changing as people increasingly live their lives online, but notes that most Canadians still want to be the ones in control of where their information ends up.

"Privacy remains an incredibly important and cherished value to Canadians – and to people around the world," the report states.

.....

By the numbers

207

Total number of formal complaints received in 2010

45

Number of complaints made about financial services companies, such as banks and credit intermediaries

42

Number of complaints in which personal information has been used or disclosed without meaningful consent

11

Complaints related to social networking, websites or Internet service providers

44

Private-sector data breaches that were voluntarily reported

1

Complaint that a bank disclosed a woman's personal information to her partner's ex-wife's lawyer

Compiled by Emily Jackson

© 2011 The Globe and Mail Inc. All Rights Reserved.

Moshonas, Jennifer

From: Dincoy, Rana
Sent: June 23, 2011 4:12 PM
To: Thompson, Julie; Moshonas, Jennifer
Subject: FW: FYI - Article on Straight.com: Online petition launched against Canadian "lawful access" bills
FYI. I was just at a talk on surveillance and public safety, organized by the Office of the Privacy Commissioner, where one of the two professors speaking referenced Lawful Access. I'll write to the whole group a bit more on it as soon as I have the chance...

Rana Dincoy
Senior Policy Analyst – Investigative Technology and Telecommunications Policy /
Analyste principale en politiques – Politique sur les technologies d'enquêtes et les télécommunications
National Security Operations Division / Division des Opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
(613)991-3240

From: Paulson, Erika
Sent: June 23, 2011 2:18 PM
To: Haeck, Kimberly; Dincoy, Rana
Cc: Burton, Meredith; Filippis, Lisa; Hawrylak, Maciek; Kwavnick, Andrea
Subject: RE: FYI - Article on Straight.com: Online petition launched against Canadian "lawful access" bills

FYI - this has been picked up on CBC.ca now:
<http://www.cbc.ca/news/technology/story/2011/06/23/technology-internet-intercept-lawful-petition.html>

Petition against internet 'lawful access' bills

Proposed rules invade privacy and boost internet costs, Open Media says

CBC News

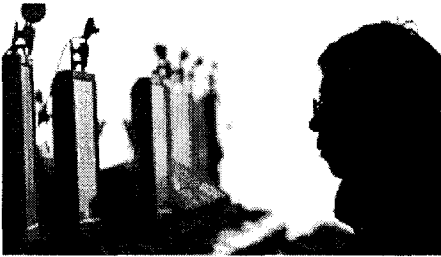
Posted: Jun 23, 2011 12:42 PM ET

Last Updated: Jun 23, 2011 1:51 PM ET

External Links

[Bill C-50](#)
[Bill C-51](#)
[Bill C-52](#)
[Conservative platform](#)
[Open Media's petition](#)

End of Supporting Story Content



The Conservatives promised as part of their election platform to reintroduce legislation tabled before the May 2 election that would give law enforcement and national security agencies up-to-date tools to fight crime in today's high-tech telecommunications environment. Associated Press

Advocates for internet users and civil liberties groups have launched a petition against proposed laws that would give police in new powers to monitor and intercept internet communications in Canada.

"These invasive surveillance bills will transform the internet to a closed, rigid, paranoid space," said Steve Anderson, executive director of Open Media, the group leading the campaign, in a statement. The group had previously mobilized internet users against usage-based internet billing.

The new "Stop Spying" petition opposes three bills that were introduced by Stephen Harper's Conservative government in the last session of Parliament, saying they will invade privacy, leave personal information less secure and boost the cost of internet service.

The Conservatives promised as part of their election platform to reintroduce legislation tabled before the May 2 election that would "give law enforcement and national security agencies up-to-date tools to fight crime in today's high-tech telecommunications environment." They committed to passing the legislation within their first 100 sitting days in office.

The bills from the last session included:

- C-50, Access to Investigative Tools for Serious Crimes Act, which would give police the power to intercept private communications without a warrant under certain circumstances.
- C-51, Investigative Powers for the 21st Century Act, which would allow police to get a) warrants to obtain information transmitted over the internet and data related to its transmission, including locations of individuals and transactions; b) orders that would compel other parties to preserve electronic evidence.
- C-52, Investigating and Preventing Criminal Electronic Communications Act, which would require internet service providers to a) have infrastructure that will allow law enforcement agents to intercept internet communications of their customers; b) provide basic information about their subscribers to law enforcement.

The government and law enforcement officials say the laws are necessary because technology provides new ways of committing crimes and makes them harder to investigate. The Conservative government has previously tried to introduce similar legislation multiple times.

Open Media said the police interception of private communications without a warrant will "invade the private lives of law-abiding Canadians." It believes the legislation will leave personal and financial information less secure and will boost the cost of internet service, since internet service providers will likely pass on the cost of installing "millions of dollars worth" of technology to make communications interceptable.

By Wednesday evening, the same day the petition was launched, 30,000 people had signed, Open Media reported.

The petition is backed by the Canadian and B.C. civil liberties associations, the Canadian Internet Policy and Public Interest Clinic at the University of Ottawa and the Tyee, a B.C.-based news and culture website. Several unions and independent media outlets are also supporting the campaign.

Erika Paulson
Tel: 613-993-4415

From: Paulson, Erika
Sent: June 23, 2011 12:16 PM
To: Haeck, Kimberly; Dincoy, Rana
Cc: Burton, Meredith; Filipps, Lisa; Hawrylak, Maciek; Kwavnick, Andrea
Subject: RE: FYI - Article on Straight.com: Online petition launched against Canadian "lawful access" bills
Importance: Low

Kimberly, Rana - FYI in Maciek and Andrea's absence.

Erika Paulson
Tel: 613-993-4415

From: Paulson, Erika
Sent: June 23, 2011 12:15 PM
To: Hawrylak, Maciek; Kwavnick, Andrea
Cc: Burton, Meredith; Filipps, Lisa
Subject: FYI - Article on Straight.com: Online petition launched against Canadian "lawful access" bills

Just caught this article. FYI in case you haven't seen. OpenMedia's press release about their online petition is here. 30562 people have signed to date: <http://openmedia.ca/news/invasive-surveillance-bills-will-cost-canadians-cash-and-civil-liberties-says-new-coalition>

Cheers,
Erika

straight.com
Vancouver's Online Source

Online petition launched against Canadian "lawful access" bills

By Yolande Cole
Publish Date: June 22, 2011

An online petition has been launched in opposition to "lawful access" legislation expected to be reintroduced by the Conservative government this fall.

OpenMedia.ca is organizing the petition against three bills that they say would violate civil liberties and translate to extra costs for Canadians.

"They allow warrantless surveillance of online activity, they're costly - Internet service providers will have to invest

000155

22/11/2011

in infrastructure, and that cost is necessarily going to be passed down to either the consumer or the taxpayer," communications manager **Lindsey Pinto** told the *Straight* by phone.

"It's essentially an antithesis to Internet openness, and we don't accept it."

The bills were introduced as C-50, C-51 and C-52 last fall but died on the order paper when the Harper government fell in March.

Pinto said they are expecting the Conservatives to reintroduce them as part of their omnibus crime legislation in September.

"We know the bills are going to be put through," said Pinto. "The Conservatives announced in their campaign platform that they were going to do so in their 100 days of their term if elected."

The bills will give the police, the Canadian Security Intelligence Service, and the Competition Bureau greater powers to intercept online communications and gather information about Internet users. The legislation will also allow law-enforcement authorities to remotely activate tracking devices found in mobile phones and GPS devices in cars.

Pinto noted the bills will require telecom providers in Canada to hand over personal information to authorities without a warrant.

"Every provincial privacy commissioner...has spoken out against this," said Pinto. "This could set a very negative precedent for surveillance in Canada, and just for the way the Internet is treated in Canada."

In March, B.C.'s information and privacy commissioner **Elizabeth Denham** and other privacy commissioners across the country wrote to the ministry of public safety to express their concerns about the "lawful access" legislation.

OpenMedia.ca is being joined by a group of over 30 other organizations, businesses and academics in challenging the bills.

You can follow Yolande Cole on Twitter at twitter.com/yolandecole.

Source URL: <http://www.straight.com/article-400631/vancouver/online-petition-launched-against-lawful-access-bills>

Erika Paulson
Senior Communications Advisor | Conseillère principale en communications
Communications - Emergency Management and National Security | Sécurité nationale et gestion des urgences
- Communications
Public Safety Canada | Sécurité publique Canada
Tel: 613-993-4415
Fax: 613-993-7062
Erika.Paulson@ps-sp.gc.ca

Scott, Marcie

From: Dincoy, Rana

Sent: June 23, 2011 4:14 PM

To: Chayer, Marie-Helene

Subject: FW: FYI - Article on Straight.com: Online petition launched against Canadian "lawful access" bills

FYI. It's now national news. At the talk I attended this afternoon, which was organized by the Office of the Privacy Commissioner and one of the speakers referenced upcoming Lawful Access legislation. I'll prepare an email on that talk as soon as possible.

Rana Dincoy

Senior Policy Analyst – Investigative Technology and Telecommunications Policy /

Analyste principale en politiques – Politique sur les technologies d'enquêtes et les télécommunications

National Security Operations Division / Division des Opérations de sécurité nationale

Public Safety Canada / Sécurité Publique Canada

(613)991-3240

From: Paulson, Erika

Sent: June 23, 2011 2:18 PM

To: Haeck, Kimberly; Dincoy, Rana

Cc: Burton, Meredith; Filippis, Lisa; Hawrylak, Maciek; Kwavnick, Andrea

Subject: RE: FYI - Article on Straight.com: Online petition launched against Canadian "lawful access" bills

FYI - this has been picked up on CBC.ca now:

<http://www.cbc.ca/news/technology/story/2011/06/23/technology-internet-intercept-lawful-petition.html>

Petition against internet 'lawful access' bills

Proposed rules invade privacy and boost internet costs, Open Media says

CBC News

Posted: Jun 23, 2011 12:42 PM ET

Last Updated: Jun 23, 2011 1:51 PM ET

External Links

[Bill C-50](#)

[Bill C-51](#)

[Bill C-52](#)

[Conservative platform](#)

[Open Media's petition](#)

End of Supporting Story Content

**Pages 158 to / à 160
are duplicates of
sont des duplicatas des
pages 154 to / à 156**

Scott, Marcie

From: Chayer, Marie-Helene
Sent: June 28, 2011 8:14 AM
To: Dincoy, Rana
Subject: RE: A talk on surveillance organized by the Office of the Privacy Commissioner of Canada (OPC)

Thanks Rana.

From: Dincoy, Rana
Sent: June 23, 2011 5:03 PM
To: Chayer, Marie-Helene; Scott, Marcie; Hawrylak, Maciek; Kwavnick, Andrea; Thompson, Julie; Moshonas, Jennifer; Emmett, Jamie
Subject: A talk on surveillance organized by the Office of the Privacy Commissioner of Canada (OPC)

I attended a very interesting talk on surveillance and public safety which was organized by the OPC. The speakers were David Wood (Sociology Professor at Queens University) and Craig Forcese (Law Professor at Ottawa U). Craig Forcese, mentioned the debate on Lawful Access he expects in Parliament, will be interesting to see because it will essentially define what is and isn't private information. According to him, while the current jurisprudence suggests that only "core" biographical information only is considered private information, the boundaries are being pushed by different actors in society. For example, the Alberta Privacy Commissioner is going to the Supreme Court to determine whether licence plates are private information.

Prof. Forcese also talked about how, from a privacy perspective, one may not wish to have divulged a piece of information which may be innocuous on its own, but put together with other information, could form a complete profile of an individual. Prof. Forcese did reference that a version of this is argument often used by govt and national security agencies ***not*** to divulge information publicly... (I have seen this argument from the OPC themselves before and can see them bringing this up at Committee.)

Both speakers admitted current laws do not really address privacy in the information age since laws are really reactive in nature. Current laws, sadly, according to both speakers, are still oriented toward defending a particular private "space", but does not address what ***information*** is private.

The main trends and issues they saw were:

- 1) Tremendously increased surveillance, by everyone: government, private industry and individuals. This is aided by the growth in smaller, cheaper and more intrusive surveillance devices. Did you know there is now a surveillance powder being tested in Japan and research is underway to make body scanners smaller? In the future, you may not even know when you're under surveillance! That possibility will erode people's trust...
- 2) Emergency of counter surveillance technology
- 3) Data warehousing is an increasing trend – the technology for data collection is slightly ahead of the technology for data analysis
- 4) Information is persistent – your information is around forever!
- 5) The border problem – server farms can be placed in countries where the privacy protections don't exist!

As for solutions, I heard the following:

- 1) International law is the ***last*** place one should go for privacy protection
- 2) Avoid having large data warehouses where all manners of information are housed together and then data-mined (FBI's database was given as an example) -- what would be preferable are smaller databases that are "firewalled" from each other
- 3) After information is collected (for let's say an investigation), purge the extraneous information after a certain amount of time. There can be set time limits, which would be renewable. This would be supervised by an independent judiciary official.
- 4) Oversight (arms-length regulator)

- 5) Compensation- make individuals who cause injury to an individual by compromising their security without good cause culpable.

Whoever is looking at potential enhancements of the privacy provisions for Lawful Access, may wish to consider 2) and 3).

I picked up the following OPC publications which may be of interest to you. I'll leave them at Kim's desk. They are:

- Deep packet inspection
- Consultations on Online Tracking, profiling and targeting, and cloud computing
- A Guide for submitting Privacy Impact Assessments to the OPC called "Expectations"
- Surveillance, Search and Seizure Powers Extended by Recent Legislation in Canada, Britain, France and the United States – Backgrounder to SECU (May 7, 2009)

Rana Dincoy

Senior Policy Analyst – Investigative Technology and Telecommunications Policy /

Analyste principale en politiques – Politique sur les technologies d'enquêtes et les télécommunications

National Security Operations Division / Division des Opérations de sécurité nationale

Public Safety Canada / Sécurité Publique Canada

(613)991-3240

Kingsley, Michèle

From: Scott, Marcie
Sent: September 12, 2011 9:54 AM
To: Kwavnick, Andrea; Hawrylak, Maciek; Kingsley, Michèle
Subject: Lawful Access Opinion Piece by BC Privacy Commissioner

Here is an opinion piece by the BC Privacy Commissioner concerning how 9/11 has changed security, and the affect this has had on privacy. It makes specific (inaccurate) reference to proposed lawful access legislation.

http://www.infomedia.gc.ca/allcontent/articles/unrestricted/2011/09/all201191322123744_4.htm

Marcie Scott

National Security Operations | Opérations de la sécurité nationale
Emergency Management and National Security Branch |
Secteur de la gestion des urgences et de la sécurité nationale
Public Safety Canada | Sécurité publique Canada

Tel: 613-949-5886

Hawrylak, Maciek

From: Hawrylak, Maciek
Sent: September 16, 2011 10:40 AM
To: Kwavnick, Andrea; Filipps, Lisa
Cc: Kingsley, Michèle; Burton, Meredith
Subject: RE: Vancouver Sun: Advocates, politicians campaign against Conservatives' proposed 'snooping law'
The actual releases from the NDP (<http://www.ndp.ca/press/ndp-gears-up-to-fight-conservatives-snooping-law>) and Green Party (<http://greenparty.ca/media-release/2011-09-15/electronic-surveillance-laws-go-too-far>).

Maciek

From: Filipps, Lisa
Sent: September 16, 2011 10:18 AM
To: Kingsley, Michèle; Kwavnick, Andrea
Cc: Burton, Meredith
Subject: FW: Vancouver Sun: Advocates, politicians campaign against Conservatives' proposed 'snooping law'

More...

From: COMDO **On Behalf Of** PSMediaCentre/CentredesmediasdeSP
Sent: Friday, September 16, 2011 10:15 AM
To: * COMMS ADG / Bureau du directeur général associé; * COMMS Communication Services Division / Division des services de communication; * COMMS DGO / Bureau de la directrice générale; * COMMS Program Communications Division / Secteur des communications de programmes; * COMMS Public Affairs Division / Secteur des affaires publiques; * Speeches / Discours; Astravas, Rutha; Beaudoin, Serge C; Bolton, Stephen; Boucher, Patrick; Boucher-Lalonde, Murielle; Cameron, Bud; Carmichael, Julie; Champoux, Elizabeth; Clairmont, Lynda; Coburn, Stacey; Crawford, Andrée; Currie, St. Clair; De Santis, Heather; DMAssistant; Duschner, Gabrielle; Dussault, Josée; Easson, Grant; Gareau-Lavoie, Genevieve; Gordon, Robert; Gow, Robert; Hitchcock, Christy; House, Andrew; Huggins, Rachel; Humeniuk, Elena; Hunt, Ryan; Jarmyn, Tom; Johnson, Mark; Kelland, Stephen; Khouri, Lisa; Kubicek, Brett; Lavoie, Micheline; Leclair, Natalie; Leclerc, Carole; Leonidis, Nelly; Lesser, Robert; MacDonald, Nicholas; MacKinnon, Paul; Marchand, Renee; McAteer, Julie; Morris, Marika; Motzney, Barbara; Mundie, Robert; Nadeau, Elisabeth; Nicole, Jean-Thomas; Oldham, Craig; Patton, Michael; Pozhke, Nicholas; Roy, Isabelle; Saunders, Joanne; Shuttle, Paul; Slack, Jessica; Stewart, Christena; Thibault, Stéphane; Tupper, Shawn; Valentin, Jason; Van Criecking, Jane; Vis, Kyle; Wex, Richard; Adam.Kates@cbsa-asfc.gc.ca; Allison.Wildgust@cbsa-asfc.gc.ca; Amitha.Carnadin@cbsa-asfc.gc.ca; Bateman, Paul; Bernard.Alladin@cbsa-asfc.gc.ca; Bindman, Stephen; Brunette, Lynn; cbsa.media@cbsa-asfc.gc.ca; Cgirouad@justice.gc.ca; Chad.Fleck@international.gc.ca; Churney, Daryl; Cobbsu@csc-scc.gc.ca; Cocking, Marie; Couture, Jocelyne; Van Allen, Elizabeth; C. Girouard; Bradley, Jolene; Mackillop, Ken; Lamothe, Maureen; Lauzon, Raymond; Lavoie, Daniel; Mailhot, Esther; Stokes, Mark; Mary.Schlosser@rcmp-grc.gc.ca; McDerby, Kate; RCMP Media Monitoring; Martin, Nadie; Robinson, N.; Rioux, Veronique; Sbinman@justice.gc.ca; Dumoulin, Stéphanie; Tim.Cogan@rcmp-grc.gc.ca; Wayne.Oakes@rcmp-grc.gc.ca
Subject: Vancouver Sun: Advocates, politicians campaign against Conservatives' proposed 'snooping law'

Advocates, politicians campaign against Conservatives' proposed 'snooping law'
September 16, 2011
Vancouver Sun, By Gillian Shaw

A grassroots Vancouver group that champions an open Internet launched an education campaign

Thursday against the Canadian government's proposed "lawful access" legislation that would give police increased power to carry out web surveillance and intercept communications.

The campaign by OpenMedia.ca drew the support of the federal Green party. And the federal New Democrats said they are "gearing up to fight the Conservatives' proposed snooping law at every level this fall in order to protect the rights and privacy of Canadians."

A series of ironic but chilling public service video advertisements produced by Vancouver's Rattlesnake Films released Thursday were drawing heavy Internet traffic.

They suggest Canadians wouldn't stand for police getting broader powers to monitor and intercept their real-world activities, from shopping to sending snail mail to chatting on the phone, but they are risking that with the proposed legislation.

The videos are the latest in OpenMedia's Stop Online Spying campaign that opposes proposed electronic surveillance laws contained in an omnibus crime bill that would give police new powers for monitoring Internet activities. The legislation has come under fire from legal and privacy experts across the country, including privacy commissioners across Canada.

"It's invasive, it's costly and the legislation is poorly thought out," said Steve Anderson, founder and executive director of OpenMedia.ca.

Anderson said the education campaign and the videos, which were produced by concerned citizens in Vancouver, were prompted by public opposition to the legislation.

"It was sort of a citizen-led initiative," said Anderson. "Canadians who know about this are upset about it."

The 2011 Canadians and Privacy Survey recently released by the Privacy Commissioner of Canada found that more than eight in 10 Canadians did not feel police and intelligence agencies should be able to request information from telecommunications companies about Canadians and their Internet usage without a warrant from the courts.

Anderson charged that the Conservative government is trying to avoid public scrutiny of the changes by including them in the omnibus bill.

"They are trying to sneak it through in this omnibus crime bill, to slide it in there without anyone knowing," he said. "It is clear there will be warrantless access to our private data. That is the rub of it all."

More than 8,000 people added their signatures to OpenMedia's Stop Online Spying petition Thursday after the campaign launch, bringing the total number on the petition started earlier this summer to 65,000.

"What we have been hearing from experts and citizens is that this new law gives the government and police way too much power to snoop into our lives," NDP privacy and digital affairs critic Charlie Angus said in the party's release from Ottawa.

"Canadians are right to feel that the Conservatives are not protecting their privacy and that we need to curb this bill."

The NDP said the legislation would legalize "widespread snooping on average citizens - all without a warrant.

"Telecom providers would also be forced to install surveillance software giving police the ability to track Internet and mobile phone activity," the party said.

A release issued by the Green party on Thursday said: "It's like having a CCTV camera in your home, and at your office watching every email you send, every phone call you make and every website you click on.

"It's creepy, it violates personal security and is inappropriate. The police should not be reading your email without a warrant first," Emma Jane Hogbin, Green party science and technology critic, said in the release.

Michael Geist, Canada Research Chair of Internet and e-commerce Law at the University of Ottawa, said despite being benignly nicknamed "lawful access," the package is not benign. In a letter to Prime Minister Stephen

Harper, a coalition of advocacy groups and professors, including Geist, outlined their concerns about the bills, including the ease "by which Canadians' Internet service providers, social networks, and even their handsets and cars will be turned into tools to spy on their activities."

[Link](#)

**Page 167
is a duplicate of
est un duplicata de la
page 168**

Hawrylak, Maciek

From: Emmett, Jamie
Sent: September 21, 2011 12:12 PM
To: Kingsley, Michèle; Kwavnick, Andrea; Hawrylak, Maciek; Scott, Marcie; Moshonas, Jennifer; Plunkett, Shawn

Subject: RE: Lawful Access in Morning Clips
Another LA article...

<http://www.cbc.ca/news/politics/story/2011/09/21/technology-internet-surveillance.html>

Jamie Emmett
613-993-7645

From: Emmett, Jamie
Sent: September 21, 2011 10:34 AM
To: Kingsley, Michèle; Kwavnick, Andrea; Hawrylak, Maciek; Scott, Marcie; Moshonas, Jennifer; Plunkett, Shawn
Subject: Lawful Access in Morning Clips

In case you hadn't already seen...

Online spying not in Tories crime package

Electronic privacy advocates expressed relief Tuesday that the Harper government's omnibus crime bill did not include measures to allow for greater spying of people's online activities, saying the omission gives them time to press for fuller debate on the issue. Canada's privacy commissioner Jennifer Stoddart and her provincial counterparts also expressed their concerns in a letter earlier this year to the **deputy minister of public safety**. They said the government's proposals would "substantially diminish" the privacy rights of Canadians and that there was "insufficient justification" for the new powers. Government officials, however, have said that authorities need "21st century tools" to fight high-tech criminals, organized crime groups and those involved in online child-sex exploitation. Windsor Star, D4 (New Brunswick Telegraph-Journal, Times & Transcript)

Page 169
is a duplicate of
est un duplicata de la
page 172

Published | Publié: 2011-09-30
Received | Reçu: 2011-09-30 5:44 AM

THE VANCOUVER SUN

VANCOUVER SUN (FINAL)
ISSUES & IDEAS, Page: A13

Lawful access would trample rights

B.C. privacy czar wants open debate on cybersnooping before law change gives police new powers

Craig McInnes, Vancouver Sun

Police need 21st century tools to fight 21st century criminals. That was the message that went along with the so-called **lawful access** legislation when it was introduced by the Conservative government in 2009.

Lawful access is the term used to describe the way police listen in on private conversations or search and seize private property, always with the authority of a warrant.

The legislation was a package of bills and amendments that the government argued are needed because cellphones and the Internet have given the bad guys new places to hide from **lawful access** and conduct their nefarious business.

Critics complained that the bills would allow police to snoop at will into the cyber-lives of Canadians without the safeguard of needing to first obtain a warrant.

Police say they aren't looking for a way to get around the need for a warrant to intercept private conversations, just the technical capacity to intercept conversations or data once a warrant has been obtained.

But privacy advocates argued that what the government was offering police was much more. The combined effect of the new rules would open a new window into our private lives that police would be able to peer through without a warrant.

In addition, the legislation would have required Internet companies to retrofit their equipment so that police could monitor in real time the activities of anyone for whom they had **lawful access** through a warrant.

That legislation was never voted on. Critics feared it would come back as part of the government's omnibus crime bill that it is now pushing through parliament after invoking closure on debate. That didn't happen, but the government is expected to reintroduce the legislation in some form soon.

B.C.'s Information and Privacy Commissioner is worried that Canadians don't really understand what is at stake.

"I see **lawful access** as one of those fundamental tipping points," Elizabeth Denham said in a telephone interview this week.

"If you are setting up private sector in a way that will provide easier access to the police, that's shifting our fundamental outlook about privacy and civil rights protections of constitutional rights."

Under the proposed changes, if police want to know what people are saying on the Internet, they will still need to get a warrant. But Internet providers would be required to turn over on request information that includes subscribers names and addresses, phone numbers, email addresses and even their ISP addresses and information about the kind of machines and software they are using.

"These appear to be minor pieces of personal information but they are personal information and it's a slippery slope to give them up without judicial oversight," Denham says.

The concern is that those pieces can be combined with information police obtain elsewhere to create personal profiles without obtaining a warrant.

Privacy advocates are also concerned about the provision that would have required private companies to build in the capacity for police to snoop in real time once they get a warrant. Large companies like Bell and Telus already have that capacity, Denham says, but small Internet providers do not.

"Do the little guys have to come up to standards of the big guys to become agents of the state? Because that's the slippery slope that we're talking about here."

Denham agrees that the police need new tools to cope with new technology. She is also not necessarily opposed to new security measures just because they erode privacy, if there is a proven benefit in return.

But Denham and other privacy commissioners in Canada say the police have yet to show any evidence that they have been thwarted in their investigations by the current **lawful access** they have to communication on the Internet.

"We would say what's the problem you are trying to solve and is there a less intrusive way to solve the same problem and I think in the case of **lawful access**, the government has not yet made its case."

cmcinnes@vancouver.sun.com ILLUS: Shannon Brady Illustration / ;

Kingsley, Michèle

From: Kingsley, Michèle
Sent: September 30, 2011 12:16 PM
To: Hawrylak, Maciek
Subject: RE: Latest LA article

Maciek - Can you pls send me the emails for Sean, Bernie, Gord, Susan.... anyone I should add to the email I'm about to send forwarding the article... thanks, m.

From: Hawrylak, Maciek
Sent: September 30, 2011 9:25 AM
To: Kingsley, Michèle; Kwavnick, Andrea
Cc: Paulson, Erika; Filipps, Lisa
Subject: Latest LA article

All,

Attached is the most recent LA article, again from today's Daily Media Summary. These are a series of technical inaccuracies, and a few things that are correct.

Perhaps most importantly, the article ends with:

"[BC Privacy Commissioner Elizabeth] Denham agrees that the police need new tools to cope with new technology. She is also not necessarily opposed to new security measures just because they erode privacy, if there is a proven benefit in return.

But Denham and other privacy commissioners in Canada say the police have yet to show any evidence that they have been thwarted in their investigations by the current lawful access they have to communication on the Internet.

"We would say what's the problem you are trying to solve and is there a less intrusive way to solve the same problem and I think in the case of lawful access, the government has not yet made its case."

Another reason to implore the operational agencies to provide us with updated stats and anecdotes on why the legislation is needed and why the current set-up is insufficient for their purposes.

Maciek

Kingsley, Michèle

From: Hawrylak, Maciek
Sent: September 30, 2011 12:22 PM
To: Kingsley, Michèle
Subject: RE: Latest LA article
Attachments: Email addresses

Emails in attachment.

Operational agency people:

Sean
Bernie
Helene
Mark
Susan

Gord

Doug

Other stakeholders:

Lisa
Andy
Matthew
Karen
Hasti

Good luck!

Maciek

From: Kingsley, Michèle
Sent: September 30, 2011 12:16 PM
To: Hawrylak, Maciek
Subject: RE: Latest LA article

Maciek - Can you pls send me the emails for Sean, Bernie, Gord, Susan.... anyone I should add to the email I'm about to send forwarding the article... thanks, m.

From: Hawrylak, Maciek
Sent: September 30, 2011 9:25 AM
To: Kingsley, Michèle; Kwavnick, Andrea
Cc: Paulson, Erika; Filipps, Lisa
Subject: Latest LA article

All,

Attached is the most recent LA article, again from today's Daily Media Summary. These are a series of technical inaccuracies, and a few things that are correct.

Perhaps most importantly, the article ends with:

"[BC Privacy Commissioner Elizabeth] Denham agrees that the police need new tools to cope with new technology. She is also not necessarily opposed to new security measures just because they erode privacy, if there is a proven benefit in return.

But Denham and other privacy commissioners in Canada say the police have yet to show any evidence that they have been thwarted in their investigations by the current lawful access they have to communication on the Internet.

"We would say what's the problem you are trying to solve and is there a less intrusive way to solve the same problem and I think in the case of lawful access, the government has not yet made its case.""

Another reason to implore the operational agencies to provide us with updated stats and anecdotes on why the legislation is needed and why the current set-up is insufficient for their purposes.

Maciek

Kingsley, Michèle

To: 'Sean Pope'; 'Bernard Tremblay'; Mark Flynn; 'Helene Van Dyke'; 'Susan Alter';
'gkirk@justice.gc.ca'; 'Douglas.Pentland@bc-cb.gc.ca'

Cc: 'Lisa.Foley@ic.gc.ca'; Andy.Kaplan-Myrth@ic.gc.ca; 'matthew.shogilev@justice.gc.ca'; 'Karen Audcent
(Karen.Audcent@justice.gc.ca)'; Kousha, Hasti

Subject: Email addresses

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

Scott, Marcie

From: Kingsley, Michèle
Sent: September 30, 2011 1:30 PM
To: 'Sean Pope'; 'Bernard Tremblay'; Mark Flynn; 'Helene Van Dyke'; 'Susan Alter'; 'gkirk@justice.gc.ca'; 'Douglas.Pentland@bc-cb.gc.ca'; 'Lisa.Foley@ic.gc.ca'; Andy.Kaplan-Myrth@ic.gc.ca; 'matthew.shogilev@justice.gc.ca'; 'Karen Audcent (Karen.Audcent@justice.gc.ca)'; Kousha, Hasti; 'bruce.wallace@ic.gc.ca'
Cc: MacDonald, Michael; Kwavnick, Andrea; Hawrylak, Maciek; Scott, Marcie; 'stan.burke@rcmp-grc.gc.ca'; 'Mollie Johnson (mollie.johnson@bc-cb.gc.ca)'
Subject: Latest LA article
Attachments: Lawful access would trample rights - Vancouver Sun 30 Sep 2011.pdf

Bonjour à tous,

Please see attached article, which interestingly quotes BC Privacy Commissioner Elizabeth Denham. She agrees that the police need new tools to cope with new technology and is not necessarily opposed to new security measures just because they erode privacy, **if there is a proven benefit in return**. "We would say what's the problem you are trying to solve and is there a less intrusive way to solve the same problem and I think in the case of lawful access, the government has not yet made its case."

This is consistent with what we're being asked at senior levels of the department.

So, this is the test to meet. We need to do some basic educating as to what BSI is, how it's used, and why it's needed. We need to demonstrate what we lose if we don't have it **as well as** what we gain by having it.

Let's meet next week to record your new data/stats and examples/anecdotes to support this (beyond child porn). We will collect and package what's provided. If you have anything to send us in the meantime, please do so. An invitation will follow.

Merci, Michèle

Michèle Kingsley

Director, Investigative Technologies and Telecommunications Policy | Directrice, Technologies d'enquêtes et politiques des télécommunications
Public Safety Canada | Sécurité publique Canada
613.949.3181 / michele.kingsley@ps-sp.gc.ca

000176

25/11/2011

**Pages 177 to / à 178
are duplicates of
sont des duplicatas des
pages 170 to / à 171**

Kingsley, Michèle

From: Kingsley, Michèle
Sent: September 30, 2011 1:38 PM
To: 'Bernard Tremblay'
Cc: Hawrylak, Maciek; Kwavnick, Andrea
Subject: RE: Latest LA article

Thanks Bernie,

We'll have the meeting late in the week.

Bonne fin de semaine.

Michèle

-----Original Message-----

From: Bernard Tremblay [mailto:Bernard.Tremblay@rcmp-grc.gc.ca]
Sent: September 30, 2011 1:38 PM
To: Douglas.Pentland@bc-cb.gc.ca; Andy.Kaplan-Myrth@ic.gc.ca; bruce.wallace@ic.gc.ca;
Lisa.Foley@ic.gc.ca; gkirk@justice.gc.ca; Karen.Audcent@justice.gc.ca;
matthew.shogilev@justice.gc.ca; Kousha, Hasti; Kingsley, Michèle; Helene Van Dyke; Mark
Flynn; Sean Pope; Susan Alter;
Cc: mollie.johnson@bc-cb.gc.ca; Kwavnick, Andrea; Hawrylak, Maciek; Scott, Marcie;
MacDonald, Michael; Stan Burke;
Subject: Re: Latest LA article

Hi Michelle,

I will be able to provide more recent examples next week. In planning the meeting, please keep in mind I will be in Quebec City next week, returning to the office on Thursday morning.

Bernie

-----Original Message-----

From: Kingsley, Michèle<Michele.Kingsley@ps-sp.gc.ca>
To: Alter, Susan <Susan.Alter@rcmp-grc.gc.ca>
To: Van Dyke, Helene <Helene.VanDyke@rcmp-grc.gc.ca>
Cc: Burke, Stan <Stan.Burke@rcmp-grc.gc.ca>
To: Tremblay, Bernard <Bernard.Tremblay@rcmp-grc.gc.ca>
To: Flynn, Mark <mark.flynn@rcmp-grc.gc.ca>
To: Pope, Sean <Sean.Pope@rcmp-grc.gc.ca>
To: Douglas.Pentland@bc-cb.gc.ca <Douglas.Pentland@bc-cb.gc.ca>
Cc: (mollie.johnson@bc-cb.gc.ca)', 'Mollie Johnson <mollie.johnson@bc-cb.gc.ca>
To: Andy.Kaplan-Myrth@ic.gc.ca <Andy.Kaplan-Myrth@ic.gc.ca>
To: bruce.wallace@ic.gc.ca <bruce.wallace@ic.gc.ca>
To: Lisa.Foley@ic.gc.ca <Lisa.Foley@ic.gc.ca>
To: gkirk@justice.gc.ca <gkirk@justice.gc.ca>
To: Audcent(Karen.Audcent@justice.gc.ca)', 'Karen <Karen.Audcent@justice.gc.ca>
To: matthew.shogilev@justice.gc.ca <matthew.shogilev@justice.gc.ca>
Cc: Kwavnick, Andrea <Andrea.Kwavnick@ps-sp.gc.ca>
To: Kousha, Hasti <Hasti.Kousha@ps-sp.gc.ca>
Cc: Hawrylak, Maciek <Maciek.Hawrylak@ps-sp.gc.ca>
Cc: Scott, Marcie <Marcie.Scott@ps-sp.gc.ca>
Cc: MacDonald, Michael <Michael.MacDonald@ps-sp.gc.ca>
Cc:
To:
To:

Sent: 09/30/2011 13:29:36
Subject: Latest LA article

Bonjour à tous,

Please see attached article, which interestingly quotes BC Privacy Commissioner Elizabeth Denham. She agrees that the police need new tools to cope with new technology and is not necessarily opposed to new security measures just because they erode privacy, if there is a proven benefit in return. "We would say what's the problem you are trying to solve and is there a less intrusive way to solve the same problem and I think in the case of lawful access, the government has not yet made its case."

This is consistent with what we're being asked at senior levels of the department.

So, this is the test to meet. We need to do some basic educating as to what BSI is, how it's used, and why it's needed. We need to demonstrate what we lose if we don't have it as well as what we gain by having it.

Let's meet next week to record your new data/stats and examples/anecdotes to support this (beyond child porn). We will collect and package what's provided. If you have anything to send us in the meantime, please do so. An invitation will follow.

Merci, Michèle

Michèle Kingsley
Director, Investigative Technologies and Telecommunications Policy | Directrice,
Technologies d'enquêtes et politiques des télécommunications Public Safety Canada |
Sécurité publique Canada
613.949.3181 / michele.kingsley@ps-sp.gc.ca<blocked::blocked::mailto:michele.kingsley@ps-
sp.gc.ca>

Hawrylak, Maciek

From: Burton, Meredith
Sent: October 3, 2011 4:35 PM
To: Kingsley, Michèle; Kwavnick, Andrea; Hawrylak, Maciek; Paulson, Erika; Kousha, Hasti
Subject: FW: RT: CTV News - Interview with Steve Anderson, Executive Director of Open Media, and Tom Stamatakis, President of the Canadian Police Association, on lawful access - 2011-10-03, 10h00 ET

Further to the link Andrea shared this morning, a transcript of an interview

From: COMDO **On Behalf Of** PSMediaCentre/CentredesmediasdeSP

Sent: Monday, October 03, 2011 4:25 PM

To: Adam.Kates@cbsa-asfc.gc.ca; Allison.Wildgust@cbsa-asfc.gc.ca; Amitha.Carnadin@cbsa-asfc.gc.ca; Bateman, Paul; Bernard.Alladin@cbsa-asfc.gc.ca; Bindman, Stephen; Brunette, Lynn; cbsa.media@cbsa-asfc.gc.ca; Cgirouad@justice.gc.ca; Chad.Fleck@international.gc.ca; Williams, Christopher; Churney, Daryl; Cobbsu@csc-scc.gc.ca; Cocking, Marie; Couture, Jocelyne; Douglas, Caroline; Van Allen, Elizabeth; C. Girouard; Bradley, Jolene; Mackillop, Ken; Lamothe, Maureen; Lauzon, Raymond; Lavoie, Daniel; Mailhot, Esther; Stokes, Mark; Mary.Schlosser@rcmp-grc.gc.ca; McDerby, Kate; RCMP Media Monitoring; Martin, Nadie; Robinson, N.; Giolti, Patrizia; Rioux, Veronique; Sbinman@justice.gc.ca; Dumoulin, Stéphanie; Tim.Cogan@rcmp-grc.gc.ca; Wayne.Oakes@rcmp-grc.gc.ca; * COMMS ADG / Bureau du directeur général associé; * COMMS Communication Services Division / Division des services de communication; * COMMS DGO / Bureau de la directrice générale; * COMMS Program Communications Division / Secteur des communications de programmes; * COMMS Public Affairs Division / Secteur des affaires publiques; * Speeches / Discours; Astravas, Rutha; Beaudoin, Serge C; Bolton, Stephen; Boucher, Patrick; Boucher-Lalonde, Murielle; Cameron, Bud; Carmichael, Julie; Champoux, Elizabeth; Clairmont, Lynda; Coburn, Stacey; Crawford, Andrée; Currie, St. Clair; De Santis, Heather; DMassistant; Duschner, Gabrielle; Dussault, Josée; Easson, Grant; Gareau-Lavoie, Genevieve; Gordon, Robert; Gow, Robert; Hitchcock, Christy; House, Andrew; Huggins, Rachel; Humeniuk, Elena; Hunt, Ryan; Jarmyn, Tom; Johnson, Mark; Kelland, Stephen; Khouri, Lisa; Kubicek, Brett; Lavoie, Micheline; Leclair, Natalie; Leclerc, Carole; Leonidis, Nelly; Lesser, Robert; MacDonald, Nicholas; MacKinnon, Paul; Marchand, Renee; McAteer, Julie; Morris, Marika; Motzney, Barbara; Mundie, Robert; Nadeau, Elisabeth; Nicole, Jean-Thomas; Oldham, Craig; Patton, Michael; Pozhke, Nicholas; Rosario, Giselle; Roy, Isabelle; Saunders, Joanne; Shuttle, Paul; Slack, Jessica; Stewart, Christena; Thibault, Stéphane; Tupper, Shawn; Valentin, Jason; Van CrieKingen, Jane; Vis, Kyle; Wex, Richard

Subject: RT: CTV News - Interview with Steve Anderson, Executive Director of Open Media, and Tom Stamatakis, President of the Canadian Police Association, on lawful access - 2011-10-03, 10h00 ET

Rough Transcript

Station: CTV News
Time/Heure: 10h00 ET
Date: 2011-10-03

Summary: *CTV News interviewed Steve Anderson, Executive Director of Open Media; and Tom Stamatakis, President of the Canadian Police Association, on lawful access.*

>> Dan: On this Monday, October the 3rd, I'm Dan Matheson. A proposed piece of legislation is stirring up concern about privacy with some people saying the powers it would grant to police go too far, an ad campaign has been launched against it. Let's take a listen, take a look. (Phone ringing).

>> Hello. Oh, hey. Hey. How's it going? Oh. Yeah, I'm still here. Yeah, how are you?

>> Jacqueline: So pretty powerful ad arguably, many would say that. In Vancouver, joining us to discuss this is Steve Anderson, executive director of Open Media.Ca as well as Tom Stamatakis, President of the Canadian Police Association. Welcome and thank you both for joining us.

>> Thanks for having me.

>> Good morning.

>> Jacqueline: Steve, maybe I'll talk to you. Talk to us about this lawful access. What is it? And, you know, what are the concerns?

>> Sure. It's a set of bills and the concern is that they would provide access to the private information of any Canadian at any time without a warrant. And so we're talking about warrantless surveillance that is invasive, costly and poorly thought out. And Canadians across the country have concerns. In fact, the government's own privacy commissioner ran a survey that found that eight out of ten Canadians -- over eight out of ten Canadians, in fact, are against providing this kind of data to police and other security officials. So clearly, Canadians are upset and, in fact, the videos that you just showed are actually produced by a Canadian for free sent to us at open media.ca and I encourage Canadians, if they aren't aware of this issue, to go to open media.ca and find out more for themselves.

>> Dan: Tom, what do you make of that, sir?

>> Well, that's not what the police community is looking for. We have profrgss (?) in the criminal code and other statutes in this country that allow for lawful access it. Does require judicial authorization for any police or law enforcement agency to access -- anyone's communication and what we're looking for --

>> Dan: Excuse me just a moment, sir. That would make it the same as a warrant, then, would it?

>> Yes, that's right. We would have to obtain some kind of authority in order to monitor anyone's communication and what we're looking for is to modernize existing provisions in the criminal code so that they keep pace with changing technology that we're dealing with today and frankly, the ad that I just saw really misleads -- is misleading to Canadians in terms of what the police community is looking for.

>> Jacqueline: Just clarify for me, how often would this be used, in what circumstance?

>> Well, we would be using these kinds of provisions, from my perspective, as a law enforcement officer, rarely. We were talking about the most serious of situations, murder investigations, distribution of child pornography, large drug trafficking files and the biggest piece of change that we're looking for is to require service providers to create an infrastructure that would allow judicial authorization, access to the kind of information that we would need in order to successfully prosecute people who are engaged in very serious criminal activity in this country.

>> Jacqueline: Mr. --

>> Dan: Mr. Anderson, that sounds pretty reasonable, I think to, a lot of Canadians. I think, wow, we got to give our cops all the tools they need to handle child pornography and to go after murderers and they need some kind of a judicial review to get this special permission. What's wrong with this?

>> Sure. I think that would be -- it would be great if that's what, in fact, the legislation suggested. If it was narrowly tailored or targeted, which is what we're asking for, that would be perfect. You know, if there was special situations where they needed to, you know, in circumstances where there was an immediate need to move quickly. That would be great. But as I said, this legislation provides law authorities with access to private information of any Canadian at any time without a warrant. And if you listen closely what Tom's saying, he's sort of avoiding that issue, and, you know, i have clause 16 right here. In front of me. And it says very clearly, every telecommunication service provider must provide law enforcement officials with name, address, telephone number, electronic mail address, internet protocol address, mobile identification number and it goes on from there. And this is all without a warrant. And there's no special targeted approach, there's no special circumstances. This is any time of any Canadian and it's warrantless.

>> Jacqueline: Mr. Anderson, we certainly don't want to prevent police in this country from not having the tools that they are saying they need, but at the same time, we want to protect our privacy as much as possible. Is there a compromise? Is there a middle ground? In other words, what if this process went ahead and then who would be monitoring it to ensure that there is no abuse here taking place? And wow agree to something like that, Mr. Anderson?

>> Sure. Well, I think that if we had a balanced reasonable approach, I think we definitely would support that and

by balance, I mean, have specific circumstances laid out like the ones that Tom suggested, where you could bypass the need for a warrant and then also have audits after the fact and make sure that those audits and that oversight covers all of the authorities that are covered under legislation. That's a reasonable approach. And I would hope that, you know, understanding that over 70,000 Canadians have signed a petition against this, eight in ten are against this legislation, I would hope that Tom and, you know, the police lobby in general would come on side and hopefully the government too will take a more reasonable and more balanced approach.

>> Dan: Steve Anderson and Tom Stamatakis.

>> Dan: More now on that proposed legislation that has been creating quite a bit of debate. Joining us in Vancouver, Steve Anderson, the Executive Director of open media.ca, and Tom Stamatakis, the president of the Canadian Police Association. If we could start with you, sir, are any other police forces enjoying the same kind of powers we're talking about here? Any templates around the world?

>> To be honest with you, I can't give you any specific examples. I know that there are similar legislation --

>> Dan: Sir, if that's the case, let me ask you this question: What situations arise now in the normal course of police work where you are stymied or in some way deprived information that this new process would help you with? Where do WE see it really helping, in what way? How Would we use it?

>> The main circumstance would be when we're dealing with organized crime, for example, if we were involved in any number of serious crimes, homicides, huge drug importation, distribution networks, where we're being stymied now is we go to seek this information from some of the service providers and the biggest challenge is they don't have the infrastructure that allows access to the information, so then we have to try and develop methodologies or technologies that will allow access. By the time we get the information, it's too late. These organizations have moved on to other things. So, you know, we're not interested in listening to what everyday Canadians talk about on cell phones or through the internet. In fact, we don't have the capacity to do that even if we wanted to. What we're talking about is serious crimes, judicial authorization for us to access the information, specifically, the kind of information that Steve mentioned earlier, and no issue with any monitoring or auditing of our activities in that regard. At all. Because it is a question of balancing, you know, public safety against privacy.

>> Jacqueline: I would like to get a reaction from Steve Anderson to some of with a you were just saying. You're saying that there's not even an ability for police to do, I guess, what the open media, the ad that we just ran, in effect, appears to imply, that you can't just go ahead and eavesdrop. Steve, can you react to that? If so, these ads would be misleading, if that's the case.

>> Yeah, well i mean, there's they're satirical ads made to stir debate but the --

>> Jacqueline: Why wow put out an ad if that's not the case, if police don't have the ability to do that, why would that be the focus of the ad?

>> Well, first of all, they will have the ability to do that. It's just --

>> Jacqueline: I think he just said they don't. They don't have that ability. Mr. Stamatakis, can you clarify? Do we have the ability?

>> We don't have the capacity. As far as I'm aware the ability to just simply on our own decide to eavesdrop on anyone's communications.

>> Jacqueline: On your own. What does that mean? What does that mean, on your own? What would that entail then? You can do it but with the assistance of others?

>> We need to have judicial authorization to eavesdrop on anybody's communication, it the no's as simple as -- as a police officer, I don't have the ability to, on my own, just arbitrarily decide to eavesdrop on somebody's internet communication or cell phone communications. It's not possible to do that. And frankly, the Canadian Association Chiefs of Police, the Canadian Association of Police Boards, have taken a position on this issue. I have not seen anywhere anyone advocate for the ability for law enforcement to look into anyone's communication except in those serious situations where there's serious crime involved and where there's a public safety component to being able to access information to prevent crime and investigate and solve crime.

>> Dan: Mr. Anderson, the question is, why would anyone, why would anybody, let alone a police officer, waste

they're time all day eavesdropping on my phone call?

>> Yeah, I don't think there's any ill intent and I think Tom's probably a good guy here. It's just the problem is that when you allow the police or other authorities to access any Canadians' information at any time without a warrant, that they can do fishing expeditions, they can sweep up people's private data when they're looking for other people, and we need to make sure that these actions are targeted, especially if we're not going to require them to use a warrant. And you can see in the legislation that, you know, I read you some of it, that that is not a very targeted approach at all. And it doesn't require a warrant, and so that's really all that we're asking for is a reasonable balanced approach where we have narrowly targeted rather than blanketed certain surveillance and blanketed data, you know, data retention and, you know, fishing expeditions.

>> Jacqueline: I want to ask you about that. I'll get your response in just a moment. I want to get from Steve Anderson what kind of response has there been to this campaign, alerting people to these new potential laws?

>> Sure. The response has been pretty great. I mean, we already knew before we put them out that eight out of ten Canadians, when asked, don't like this legislation, don't want the police to have a warrantless access to their private information. So, you know, it's not surprising that Canadians ran with it. Over a hundred thousand people have watched these videos. And again, they're produced by everyday Canadians who came to us and said, you know, check out these videos. And then we put them out on the web and they went viral. Now --

>> Jacqueline: We're out of time. So I just want to -- if you could make a short comment and then we'll have to wrap it up. I appreciate the time.

>> Well, the organization that I represent and none of the other law enforcement organizations that I refer to, I haven't seen them put any position forward that suggests that we should be able to access information without a warrant.

>> The legislation's in there.

>> Jacqueline: Obviously we're going to be talking about this debate for some time to come. It's good obviously for Canadians to get more acquainted with the issue because it will continue. So Tom Stamatakis with the Canadian Police Association and Steve Anderson with open media.ca. Good of you to both to join us.

Due to the nature of closed captioning, grammatical and editorial errors may be found within the attached transcript. Étant donné la nature du sous-titrage, il peut y avoir des erreurs grammaticales et de rédaction dans la transcription ci-attachée.

Questions? Please contact us at PSMediaCentre/CentredesmediasdeSP@ps-sp.gc.ca.

Questions? Veuillez communiquer avec nous au PSMediaCentre/CentredesmediasdeSP@ps-sp.gc.ca.

Scott, Marcie

From: Kwavnick, Andrea
Sent: October 5, 2011 8:07 AM
To: Kousha, Hasti
Cc: Scott, Marcie
Subject:
Attachments:

Hi Hasti,

Thanks
Andrea

**Pages 186 to / à 190
are withheld pursuant to section
sont retenues en vertu de l'article**

**of the Access to Information
de la Loi sur l'accès à l'information**

Scott, Marcie

From: Kwavnick, Andrea
Sent: October 12, 2011 8:40 AM
To: Hawrylak, Maciek; Scott, Marcie; Kingsley, Michèle; Kousha, Hasti
Subject: LA - article

Interesting article. The main problem I see is that there is no discussion/explanation of what is considered to be 'private data.' The work Marcie is doing on BSI and reasonable expectation of privacy will be important in this regard.

The new rules would require **Canadian** telecommunications firms to install mechanisms to make it easier for the government to collect private data.

Online privacy under scrutiny in the U.S.

Google hands over personal information of WikiLeaks volunteer

John Terauds **Toronto Star**

United States government seizures of personal information could foreshadow similar moves in **Canada**, if the federal government introduces new privacy legislation.

The Wall Street Journal reported Sunday that Google and Sonic, an Internet service provider, handed over the IP address and two years worth of email contacts for computer security expert and WikiLeaks volunteer Jacob Appelbaum to the United States justice department of without a search warrant.

Online reaction divided among those who support new state powers to fight crime and **terrorism**, and those who insist that judges must decide when and how private information can be tapped.

Justice department actions have prompted lawsuits claiming that the U.S. Electronic Communications Privacy Act of 1986, contravenes constitutional protections from unlawful search and seizure.

In one case, a U.S. District Court ruled last December that the government violated the Fourth Amendment when it seized 24,000 emails without a warrant.

Google reports that it received 4,601 requests for personal data from the U.S. government in the last six months of 2010, complying with 94 per cent of those requests. It does not specify how many were accompanied by warrants.

"Our goal is to provide our users access to information and to protect the privacy of our users." Google states in its report. "Whenever we receive a request, we first check to make sure it meets both the letter and the spirit of the law before complying."

Despite this, Google and many Internet service providers do not like that such government requests cannot be disclosed to customers.

Currently, **Canadians'** online privacy is protected by the Personal Information Protection and Electronic Documents Act of 2004. But the federal government has indicated that it wants to make it easier for investigators to check email and mobile device data.

Public Safety Minister Vic Toews said in a press scrum last week that, "We are going to move ahead with the **lawful access** legislation." His office did not respond to a request for timing.

The new rules would require **Canadian** telecommunications firms to install mechanisms to make it easier for the government to collect private data.

"We believe that there is insufficient justification for the new powers," wrote the country's privacy commissioners in an open letter to the deputy **minister of public safety** last March. ILLUS: **Vic Toews, minister of public safety**, said last week Ottawa was moving ahead with **lawful access** legislation.

Kwavnick, Andrea

From: Christopher Prince [Christopher.Prince@priv.gc.ca]
Sent: October 21, 2011 12:17 PM
To: Kwavnick, Andrea
Subject: links

Good morning Ms. Kwavnick,

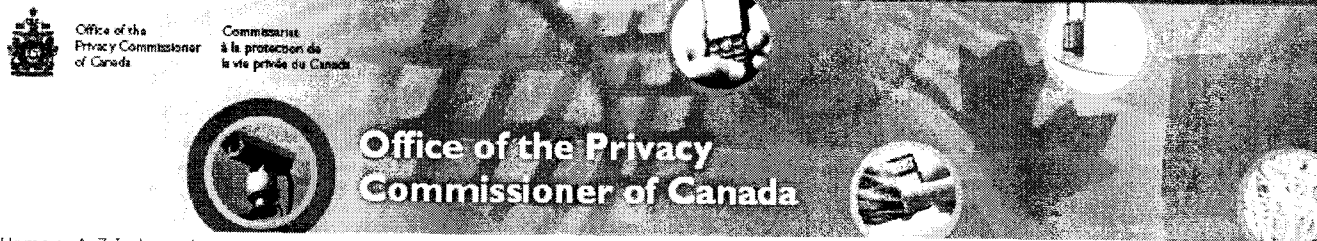
It was very nice to meet you yesterday afternoon.

I thought I should point out that we actually have a section on our site that pull together the public work we've done on lawful access - http://www.priv.gc.ca/a-z/L/index_e.cfm - or at least the major materials from the past ten years.

And of course, if you have any other follow-up questions, please just let me know.

Hope you have a nice weekend.

Chris Prince
Strategic Policy Analyst
Office of the Privacy Commissioner of Canada
112 Kent Street, 3rd Floor
Ottawa, Ontario
K1A 1H3
(613) 947-7005



Home > A-Z Index > L

A-Z Index - L

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)

Lawful Access Proposals

Letter to Minister of Public Safety Vic Toews - October 27, 2011

News Release: Privacy Commissioner outlines concerns about potential lawful access legislation - October 27, 2011

Letter to Public Safety Canada from Canada's Privacy Commissioners and Ombudspersons on the current 'Lawful Access' proposals - March 9, 2011

Speech: A secure society: Meshing privacy and public safety - January 21, 2011

Letter to the Standing Committee on Public Safety and National Security regarding the Commissioner's initial analysis on the privacy implications on Bills C-46 and C-47 - October 27, 2009

"Protecting Privacy for Canadians in the 21st Century" - Resolution of Canada's Privacy Commissioners and Privacy Enforcement Officials on Bills C-46 and C-47 - September 9-10, 2009, St. John's, Newfoundland and Labrador

Backgrounder: Surveillance, Search or Seizure Powers Extended by Recent Legislation in Canada, Britain, France and the United States - May 7, 2009

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

Response to the Government of Canada's "Lawful Access" Consultations (May 5, 2005)

Appearance before the Subcommittee on National Security of the Standing Committee on Justice and Human Rights - February 10, 2003

Letter from David Loukidelis, Information and Privacy Commissioner for British Columbia - October 3, 2002

Letter from David Loukidelis to the Prime Minister - January 29, 2003

Letter to Minister of Justice and Attorney General of Canada - November 25, 2002

News Release - Letter to the Honourable Martin Cauchon, Minister of Justice and Attorney General of Canada - November 25, 2002

Legal Opinions

Opinion - Pretexting and Bill C-27 - David M. Paciocco - April 26, 2009

Opinion by Justice La Forest - April 10, 2002

Opinion by retired Supreme Court Justice Hon. Gérard V. La Forest, C.C., Q.C. - November 22, 2002

Opinion by Mr. Roger Tassé, O.C., Q.C. - November 22, 2002

Opinion by Marc Lalonde, P.C., O.C., Q.C. - January 9, 2003

Legislation

The Privacy Act

The Personal Information Protection and Electronic Documents Act (PIPEDA)

Date Modified: 2011-11-25

Kwavnick, Andrea

From: Christopher Prince [Christopher.Prince@priv.gc.ca]
Sent: October 26, 2011 10:47 AM
To: Kwavnick, Andrea
Subject: RE: links

Andrea,

I suspect for your specific question, the last section of this letter:
http://www.priv.gc.ca/parl/2009/let_091027_e.cfm offers the most concrete detail. We
tend to carry that set of messages with us everywhere on this issue. And your colleague
from PS' cybersecurity unit too - we'd exchanged emails on another project but never met.
In any event it was very nice good to have you there for the discussion.

All the best,
Chris

-----Original Message-----

From: Kwavnick, Andrea [mailto:Andrea.Kwavnick@ps-sp.gc.ca]
Sent: Tuesday, October 25, 2011 4:06 PM
To: Christopher Prince
Subject: RE: links

Hi Chris,

Thanks for sending the link. This type of information is always useful.

Likewise if you have any questions, please don't hesitate to get in touch.

Thanks
Andrea

Andrea Kwavnick
Senior Policy Advisor/Conseiller principal en politiques National Security
Technologies/Technologies de Sécurité Nationale National Security Operations/Opérations
de la Sécurité Nationale Public Safety Canada/Sécurité Publique Canada
tel: 613.949.6169
Andrea.Kwavnick@ps-sp.gc.ca

-----Original Message-----

From: Christopher Prince [mailto:Christopher.Prince@priv.gc.ca]
Sent: October 21, 2011 12:17 PM
To: Kwavnick, Andrea
Subject: links

Good morning Ms. Kwavnick,

It was very nice to meet you yesterday afternoon.

I thought I should point out that we actually have a section on our site that pull
together the public work we've done on lawful access - http://www.priv.gc.ca/a-z/L/index_e.cfm - or at least the major materials from the past ten years.

And of course, if you have any other follow-up questions, please just let me know.

Hope you have a nice weekend.

Chris Prince
Strategic Policy Analyst
Office of the Privacy Commissioner of Canada
112 Kent Street, 3rd Floor

Ottawa, Ontario
K1A 1H3
(613) 947-7005



Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada



Office of the Privacy Commissioner of Canada

Home > Parliamentary Activities > Appearances before Parliamentary Committees

Parliamentary Activities

Appearances before Parliamentary Committees

Select Year

Privacy Act Reform

PIPEDA Review

Appearances before Parliamentary Committees

Letter regarding the Commissioner's initial analysis on the privacy implications on Bills C-46 and C-47

The Privacy Commissioner of Canada, Jennifer Stoddart, sent the following letter to the Standing Committee on Public Safety and National Security, regarding her initial analysis on the privacy implications on Bills C-46, the Investigative Powers for the 21st Century Act (IP21C), and C-47, the Technical Assistance for Law Enforcement in the 21st Century Act (TALEA)

October 27, 2009

Mr. Garry Breitkreuz, MP
Chair of the Standing Committee on Public Safety and National Security
131 Queen Street – 6th floor
House of Commons
Ottawa, Ontario K1A 0A6

Dear Mr. Breitkreuz:

I am writing to provide the members of the Standing Committee on Public Safety and National Security with some preliminary views on the privacy implications stemming from Bills C-46 and C-47. As you are aware, I am often called upon to comment on legislation that will result in new or expanded forms of personal information being collected by federal government institutions. Those views, and analysis conducted by my Office, are specifically undertaken to support the deliberations of Parliament.

It must be stated at the outset that we recognize the concerns of law enforcement and national security authorities with the speed of developments in information technology and the anonymity they afford. Bills C-46 and C-47 seek to address the consequent public safety challenges and that objective is valid. That said, whenever new surveillance powers or programs are proposed, it is my view that there must be demonstrated necessity, proportionality and effectiveness. They should also be the least-invasive alternative available. These tests are all the more important in the area of public safety, as the use of surveillance powers by authorities can have deep and lasting impact on peoples' lives.

The consequences for individuals as their personal information is collected and shared among authorities in various countries can escalate far beyond the initial objectives of public safety. Recent international reports, Canadian court rulings and federal commissions of inquiry have shown this clearly. Proper protections for privacy in this area reside in the strict limitation of invasive powers to what is demonstrably necessary to ensure public safety and in strong measures for accountability, commensurate with the powers vested. It is a matter of protecting human rights and assuring public trust.

Taking into account the real challenges of law enforcement and national security agencies in the Internet age and the fundamental right to privacy that underpins our democratic society, and after careful study and extensive consultation this past summer, I have concluded that elements of the proposed legislation raise significant privacy concerns. These must be addressed by proponents of the bills.

I would draw to the attention of this Committee, and all Parliamentarians, that the proposed legislation contains many provisions that would increase the level of access by law enforcement and national security authorities to personal information. In that regard, it is important that Parliament be satisfied that:

- The need for these provisions has been clearly demonstrated,
- The lowered legal requirements for use of invasive powers is justified,
- The lessons of similar initiatives in other countries are considered, and
- The oversight, reporting and accountability mechanisms are carefully calibrated, to ensure they mirror the breadth and scope of new powers

Analytical approach and consultations

It is important to note that our Office approached the examination of both pieces of legislation with fresh eyes and an open mind. While previous iterations or initiatives – like the 1999 Justice Canada initiative, the 2005 public consultation or the 2007 Public Safety request for submissions on Customer Name and Address access – may have served as background, they did not colour our analysis. Instead, since the legislation was tabled this past summer, our Office carefully read and analysed the two bills anew.

We also wanted to hear from informed experts, therefore between June and September of this year, my staff met with representatives of Justice Canada and Public Safety Canada, provincial privacy commissioners, the telecommunications industry (manufacturers, service providers and associations), law enforcement (RCMP and the Canadian Association of Chiefs of Police), civil society groups, academic specialists, as well as subject experts in the fields of information policy, network security, criminal law and intelligence operations. These conversations helped our Office identify the privacy issues raised by the two bills, which relate to the following areas:

Necessity: Though isolated anecdotes abound, and extreme incidents are generally referred to, no systematic case has yet been made that demonstrates a need to circumvent the current legal regime for judicial authorization to obtain personal information. Before all else, law enforcement and national security authorities need to explain how the current provisions on judicial warrants do not meet their needs.

Necessity given international obligations: A principal rationale cited for the need to update Canada's interception and surveillance regime – as proposed in C-46 and C-47 – is ratification of the Council of Europe *Convention on Cybercrime*. However, many of the powers introduced in the proposed legislation go far beyond the legal requirements of the Convention. Our analysis would suggest that Canada has already met most of the substantive legal changes required. Certainly some caution should be exercised, given the fact that similar legal initiatives in the US and UK led to significant concerns in relation to privacy.

Proportionality of thresholds: Canadian law imposes rigorous thresholds of evidence for authorities to obtain access to personal information. They form the heart of protections that Parliament put in place to protect privacy in Canada. The downward movement from *reasonable grounds to believe* to *reasonable grounds to suspect* in some cases (for some production orders) - or to no threshold of evidence at all (for

subscriber data access) - must be shown to be a proportionate response to safety and security imperatives. As it stands, the new powers envisaged are not limited to a specific range or seriousness of criminality, or to a specific level of urgency. In the case of Bill C-47, there is not even a requirement for the commission of a crime to justify access to personal information without a warrant. The onus lies with proponents of the legislation to demonstrate the need for lowered thresholds to obtain personal information.

Proportionality of oversight and review mechanisms: Only prior court authorization serves as rigorous privacy protection. Should Parliament allow law enforcement and national security authorities to circumvent the courts to obtain personal information, the corresponding oversight mechanisms must be established. My Office is clearly implicated at several points in Bill C-47, wherein my staff may review the records created by officers at the RCMP or Competition Bureau as they exercise new powers. Given the scale envisaged, with upwards of thousands of individuals in the RCMP alone potentially empowered to access subscriber data, it would be difficult for us, within our current resources, to offer any assurance to

Parliamentarians or Canadians of proper auditing. Still, review after the fact arrives too late. Privacy has already been breached, it is difficult to properly assess the circumstances, and there is no remedy for the ultimate outcome of the breach.

Demonstrated effectiveness through clear public reporting and accountability: In Bill C-47, audits are conducted internally and not required annually, while follow-up reporting to the responsible Minister and my Office are discretionary, as opposed to regular requirements. This will not afford objective, timely assessment of privacy risks or breaches. It is my view that, should the powers envisaged be granted, copies of those reports from the RCMP and Competition Bureau should be provided to the Minister and my Office on an annual basis. My audit and review staff can then proceed accordingly.

Flowing from these concerns, we would look forward to a constructive dialogue with the Committee on the following points or alternatives:

Examine warrant provisions in the Criminal Code. Rather than creating blanket, open access for authorities to search subscriber data, as in Bill C-47, there are other investigative options or legal changes to consider. Emergency provisions to conduct search, seizure or interception without a warrant in exigent circumstances are already in the *Criminal Code*. A similar provision for production and assistance orders should be considered to address the issue police have described in obtaining data.

Review the process for court authorization in Canada. If the underlying problem resides in Canada's current warrant system, this is where the government's attention should be directed, as opposed to limiting court oversight. Law enforcement and national security authorities should state the shortcomings they identify in the court warrant system so they can be addressed to adapt the system to the new challenges of the Internet age rather than sacrifice the principles that underpin the very society we seek to protect.

Tailor the scope of new powers. Any regime that circumvents court authorization raises significant privacy issues. If Parliament chooses to grant the proposed powers, they must be restricted in their application to the investigation of crimes or threats where such an invasion of privacy is justified. That is the Canadian legal tradition.

Revisit oversight regime. Internal audit, reporting with self-discretion and the role of external review bodies need to be strengthened with provisions for specific reporting requirements, regular review, dedicated resources for oversight and transparent mechanisms for accountability to assure the Canadian public.

Parliament should consider a five-year review for Bill C-46. While Bill C-47 has such a provision, Bill C-46 would also merit close review by Parliament, given how the two pieces of legislation interact. These reviews should be conducted with an eye to demonstrated evidence of effectiveness, minimal invasion of privacy and clear operation within bounds of the law.

Letter to the Standing Committee on Public Safety and National Security regarding the C-46 and C-47

Require annual public reporting. Yearly statistics on the use, results and effectiveness of new powers (subscriber data requests, preservation demands, tracking warrants, etc.) should be required by statute. Besides bolstering accountability, these reports would usefully support Parliament's five-year review of the powers.

Review the regulations flowing from both bills. Given the important administrative, procedural and technical details involved, Parliament should conduct full committee reviews and hear from all interested stakeholders on both legislation and regulations. This should occur before either bill comes into force.

In summary, we urge Parliament to review Bills C-46 and C-47 in light of the following questions:

- In specific terms, how is the current regime of judicial authorization not meeting the needs of law enforcement and national security authorities in relation to the Internet?
- What law enforcement or national security duty justifies access without a warrant by authorities to personal information or preservation of private communication?
- Why are some of these powers unrestricted, when the spirit of Canadian law clearly reflects the view that access or seizure without court authorization should be exceptional?
- And finally, are the mechanisms for accountability commensurate to the unprecedented powers envisaged?

Based on this initial analysis, my Office will be preparing a full submission for your consideration, in anticipation of your Committee's study of the legislation. Given the public interest in this issue, we anticipate posting this letter on our website in the near future. I would like to thank you for your attention to this critical issue and look forward to discussing the initiative further when meetings on the bills commence.

Sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

cc: Honourable Robert Nicholson, Minister of Justice
Honourable Peter Van Loan, Minister of Public Safety
Paul Szabo, Chair of the Standing Committee on Access to Information,
Privacy and Ethics (ETHI)
Roger Préfontaine, Clerk of the Committee (SECU)
Jacques Maziade, Clerk of the Committee (ETHI)

Date Modified: 2009-10-29

Scott, Marcie

From: Kwavnick, Andrea
Sent: October 21, 2011 4:34 PM
To: Kingsley, Michèle
Cc: Hawrylak, Maciek; Moshonas, Jennifer; Scott, Marcie; Emmett, Jamie; Plunkett, Shawn; Durand, Mathieu; Haeck, Kimberly
Subject: Security/Privacy Discussion at Carleton

Michèle,

Yesterday afternoon I attended a discussion at Carleton University. The session was entitled 'Privacy and Security: Recent Developments and Future Implications for New Government Surveillance Powers' and the speaker was Chris Prince (Senior Policy Analyst at the OPC). The event was put on by the Canadian Centre for Intelligence and Security Studies.

Overall I found the presentation to be fairly balanced. Only once did he say something that was inaccurate, but I corrected him (more on that later). There weren't more than a dozen people in the audience, mostly students and one analyst from the Cyber Security Directorate.

Presentation highlights:

- He spoke about how the definitions of privacy and security have 'slippery slopes' but that they don't need to be mutually exclusive.
- He talked about some of the new technologies and policies that can impact privacy - ie: facial recognition, CCTV, the US monitoring all travelers that travel in US airspace, even though they may not land in the US

Then onto Lawful Access:

- He provided a timeline starting with the SolGen Standards in 1995 up to the Bills being introduced and then dying on the Order Paper in 2011

- Former Bill C-50 - he called the Bill 'pragmatic' and gave the gov't credit for "getting it right" in that the Bill would simplify the warrant application process by creating a single application process; he was also pleased that the former Bill included annual reporting requirements for emergency wiretaps

- Former Bill C-51 - he said the Bill "stretched" beyond the requirements of the Cybercrime Convention. He said that the Cybercrime Convention includes 30 requirements but that 28 of them are already included in the *Criminal Code*. The only two not already in the Code are: 1) date preservation and 2) real time access to traffic. I haven't verified his math or examined whether C-51 does in fact go beyond the Convention, but that is something we could look into. He also said the Bill should have a 5 year Parliamentary review - as does C-52.

- Former Bill C-52 - his main focus of the Bill was s.16 - there was almost no mention of the intercept capability component. He explained what PIPEDA does and the confusion surrounding the term 'lawful authority' but noted that PIPEDA amendments would clarify that the term does not mean a warrant/judicial authority. However, he did not explicitly say that authorities today can already access this info without a warrant. He commented that the Bill included "20 or 25 identifiers" and that TSPs are trying to figure out how they will collect and gather all of these identifiers. I clarified that the Bill includes 11 identifiers and that TSPs would only be required to provide those that are in their possession and control - and would not be required to start collecting these identifiers. There was no discussion as to what the identifiers can/cannot do or what is considered 'private information.'

He made a comment that the review mechanisms in C-52 were lacking. After the presentation I spoke with him and asked in what way they were lacking. He provided the following ways to improve the review aspect of the Bill:

000202

25/11/2011

- conduct annual audits - as opposed to regular audits
- remove the discretionary element to the audit reports
- he raised the issue that the OPC may not have the resources and expertise to review/audit the RCMP with respect to subscriber information, and that this responsibility should be with the RCMP Complaints Commission. From the way he spoke I think this may be his own idea and does not necessarily reflect OPC thinking
- he raised the issue of the Provinces not having the resources necessary to review the provincial police forces. I explained that because of fed/prov jurisdictional issues the most we could do was have the OPC - in her annual report to Parliament - note the mandates of her provincial counterparts and highlight any deficiencies.

Chris sent me an email this afternoon with the link to the LA-related material on the OPC website (http://www.priv.gc.ca/a-z/L/index_e.cfm) and opened the door for follow-up discussions.

Thanks
Andrea

Scott, Marcie

From: Kousha, Hasti
Sent: October 24, 2011 3:18 PM
To: Scott, Marcie
Subject: RE:
Attachments:

Hi Marcie,

Thank you,
Hasti

Hasti Kousha
Legal Counsel/Avocate
Public Safety Canada Legal Services/Services juridiques Sécurité publique Canada
269 Laurier Avenue West/269, avenue Laurier Ouest
Ottawa, Ontario
Telephone/Téléphone: 613-949-9927
Facsimile/Télécopieur: 613-990-8307
Email/Courriel: hasti.kousha@ps-sp.gc.ca

SOLICITOR-CLIENT PRIVILEGE/SECRET PROFESSIONNEL DE L'AVOCAT

From: Scott, Marcie
Sent: October 19, 2011 9:12 AM
To: Kousha, Hasti
Subject: RE:

Great, thanks!

Marcie Scott
613-949-5886

From: Kousha, Hasti
Sent: October 18, 2011 6:13 PM
To: Scott, Marcie
Subject: Re:

Hi Marcie,

Thanks,
Hasti

From: Scott, Marcie

000204

25/11/2011

Sent: Tuesday, October 18, 2011 05:09 PM
To: Kousha, Hasti
Subject: RE:

Hi Hasti,

Thank you!

Marcie Scott
613-949-5886

From: Scott, Marcie
Sent: October 7, 2011 4:56 PM
To: Kwavnick, Andrea; Kousha, Hasti
Subject: RE:

Hi Hasti,

Have a great weekend!

Marcie Scott
613-949-5886

From: Kwavnick, Andrea
Sent: October 5, 2011 10:49 AM
To: Kousha, Hasti
Cc: Scott, Marcie
Subject: RE:

Thanks Hasti.

Andrea

From: Kousha, Hasti
Sent: October 5, 2011 10:19 AM
To: Kwavnick, Andrea
Cc: Scott, Marcie
Subject: RE:

Hi Andrea,

Thanks,
Hasti

From: Kwavnick, Andrea
Sent: October 5, 2011 8:07 AM
To: Kousha, Hasti
Cc: Scott, Marcie

000205

25/11/2011

Subject:

Hi Hasti,

Thanks
Andrea

**Pages 207 to / à 212
are withheld pursuant to section
sont retenues en vertu de l'article**

**of the Access to Information
de la Loi sur l'accès à l'information**

**Pages 213 to / à 214
are not relevant
sont non pertinentes**

**Pages 215 to / à 217
are duplicates of
sont des duplicatas des
pages 224 to / à 226**

Hawrylak, Maciek

From: Hawrylak, Maciek
Sent: October 27, 2011 12:22 PM
To: Kingsley, Michèle
Cc: Kwavnick, Andrea
Subject: RE: HEAD'S UP: CBC request re: privacy commissioner's letter

Michele,

Here are the lines. Andrea has provided input:

Proposed Lines

- Our Government remains committed both to giving police the tools they need to do their job, and strongly protecting the privacy rights of Canadians.
- The proposed measures would fix the problem that occurs when the police and CSIS are unable to intercept communications because of a lack of intercept capable equipment at the service provider.
- The Courts will continue to review and authorize requests to intercept communications, except in exigent circumstances, as is the case today.
- Today, basic subscriber information can be requested without judicial authorization under the *Personal Information Protection and Electronic Documents Act*. The proposed measures continue this practice of allowing authorities to access this information without a warrant.
- The proposed measures would actually strengthen the accountability of the current subscriber information regime by introducing robust recording, reporting, and audit requirements, none of which exist today.

And the old lines, for comparison:

- As technology evolves, many criminal activities – such as the distribution of child pornography - become much easier.
- We are proposing measures to bring our laws into the 21st Century and provide police with the tools they need to do their job.
- Our approach strikes an appropriate balance between the investigative powers used to protect public safety and the necessity to safeguard the privacy of Canadians.

I note that the old lines, which presumably have already been released, say “We are proposing measures”, which suggests this is definitely coming forward, so I've adopted the same approach.

Maciek

From: Kingsley, Michèle
Sent: October 27, 2011 11:54 AM
To: Hawrylak, Maciek
Subject: FW: HEAD'S UP: CBC request re: privacy commissioner's letter

Maciek - Can you have something soon? m

From: Filippis, Lisa
Sent: October 27, 2011 11:51 AM
To: Kingsley, Michèle; Paulson, Erika; Kwavnick, Andrea; Hawrylak, Maciek
Cc: MacDonald, Michael; Burton, Meredith; Wilson, Barbara; Slack, Jessica
Subject: Re: HEAD'S UP: CBC request re: privacy commissioner's letter

000218

24/11/2011

Thanks - we have a new call from the National Post and MO is receptive to getting some messages from you - Barb Wilson will be in touch.

From: Kingsley, Michèle
Sent: Thursday, October 27, 2011 11:45 AM
To: Filipps, Lisa; Paulson, Erika; Kwavnick, Andrea; Hawrylak, Maciek
Cc: MacDonald, Michael; Burton, Meredith; Wilson, Barbara; Slack, Jessica
Subject: RE: HEAD'S UP: CBC request re: privacy commissioner's letter

We will send you responsive lines that could have been used and could be used for future similar pieces.

From: Filipps, Lisa
Sent: October 27, 2011 11:15 AM
To: Kingsley, Michèle; Paulson, Erika; Kwavnick, Andrea; Hawrylak, Maciek
Cc: MacDonald, Michael; Burton, Meredith; Wilson, Barbara; Slack, Jessica
Subject: Re: HEAD'S UP: CBC request re: privacy commissioner's letter

I think that is likely closed for this call but I think our MO need some key points we could clarify for other calls. I would be happy to try to get some additional msgs up to them.

From: Kingsley, Michèle
Sent: Thursday, October 27, 2011 11:09 AM
To: Paulson, Erika; Kwavnick, Andrea; Hawrylak, Maciek
Cc: MacDonald, Michael; Burton, Meredith; Filipps, Lisa; Wilson, Barbara; Slack, Jessica
Subject: RE: HEAD'S UP: CBC request re: privacy commissioner's letter

Is there an opportunity to respond further? Or is the MO response pretty much it? Because we could respond directly to some points - such as her claim that we're lowering the threshold for BSI, which we're not... there are more... Do we have a window?

From: Paulson, Erika
Sent: October 27, 2011 11:02 AM
To: Kwavnick, Andrea; Hawrylak, Maciek
Cc: Kingsley, Michèle; MacDonald, Michael; Burton, Meredith; Filipps, Lisa; Wilson, Barbara; Slack, Jessica
Subject: HEAD'S UP: CBC request re: privacy commissioner's letter

Hi Andrea and Maciek,
Just a head's up that our issues management team received a request from CBC to respond to an open letter RE Lawful Access from the Privacy Commissioner to Minister Toews (please find link here: http://www.priv.gc.ca/media/nr-c/2011/let_111027_e.cfm#contenttop).

MO has responded with the following lines:

- As technology evolves, many criminal activities – such as the distribution of child pornography - become much easier.
- We are proposing measures to bring our laws into the 21st Century and provide police with the tools they need to do their job.
- Our approach strikes an appropriate balance between the investigative powers used to protect public safety and the necessity to safeguard the privacy of Canadians.

Also note: the Privacy Commissioner tweeted the letter in the last 15 minutes to over 3000 followers. We are already seeing retweets of it.

000219

24/11/2011

TWEET:

PrivacyPrivee Privacy Commission

#Privacy Commissioner outlines concerns about potential lawful access legislation. Letter to Minister of @Safety Canada <http://bit.ly/tqa78K>

Thanks,
Erika Paulson
613-993-4415

Reporter's Name

Media Outlet CBC Online

Call Date 10/27/2011 11:00 AM

Telephone

E-mail address @cbc.ca

Deadline 10/27/2011 5:00 PM

Status Consulting

Branch NS

Subject Lawful Access

Questions I was wondering if I could get a response from Minister Toews to Privacy Commissioner Jennifer Stoddart's letter about lawful access:

http://www.priv.gc.ca/media/nr-c/2011/let_111027_e.cfm#contenttop

I'm posting a story shortly and will add your response as soon as I receive it.

From: @CBC.CA]

Sent: Thursday, October 27, 2011 10:23:55 AM

To: PS Media Relations / Relations médias SP

Subject: CBC request re: privacy commissioner's letter

Auto forwarded by a Rule

Hi there,

I was wondering if I could get a response from Minister Toews to Privacy Commissioner Jennifer Stoddart's letter about lawful access:

http://www.priv.gc.ca/media/nr-c/2011/let_111027_e.cfm#contenttop

I'm posting a story shortly and will add your response as soon as I receive it.

Thanks so much,

000220

24/11/2011

Emily.

CBCNews.ca
cbc.ca/technology
emily@cbc.ca

MacDonald, Michael

From: Filipps, Lisa
Sent: October-27-11 12:26 PM
To: Kingsley, Michèle; Wilson, Barbara
Cc: Slack, Jessica; Hawrylak, Maciek; Kwavnick, Andrea; MacDonald, Michael
Subject: RE: proposed lines with additions from former C-52

Michele – the National Post call has been closed but MO is still open to receiving information.

From: Kingsley, Michèle
Sent: Thursday, October 27, 2011 11:57 AM
To: Wilson, Barbara
Cc: Filipps, Lisa; Slack, Jessica; Hawrylak, Maciek; Kwavnick, Andrea; MacDonald, Michael
Subject: RE: proposed lines with additions from former C-52

Thanks. We'll get back to you.

From: Wilson, Barbara
Sent: October 27, 2011 11:56 AM
To: Kingsley, Michèle
Cc: Filipps, Lisa; Slack, Jessica
Subject: proposed lines with additions from former C-52

Michèle,

Here's a proposed set of lines re Lawful Access and response to Privacy Commissioner's letter online to PS which combines MO's previously used lines (first three bullets) with three additional ones that correct the misinformation that's currently circulating about warrant-less access.

Keeping in mind MO preference for to-the-point lines, I'm happy to take suggestions.

Thank you

- As technology evolves, many criminal activities – such as the distribution of child pornography - become much easier.
- We are proposing measures to bring our laws into the 21st Century and provide police with the tools they need to do their job.
- Our approach strikes an appropriate balance between the investigative powers used to protect public safety and the necessity to safeguard the privacy of Canadians.
- Under the proposed legislation, the Courts **will continue to review and authorize** requests to intercept the content of communications, except in exigent circumstances, as is the case today.

- The legislation would also require that telecommunications service providers supply **designated** persons with basic subscriber information upon request.
- Current legislation allows service providers to provide authorities with basic subscriber information. However, this is carried out in an *ad hoc* manner, with some service providers assisting officials, and others not. Furthermore, there is no system of accountability to ensure the information is accessed properly. The proposed legislation will address that.

Barbara Wilson
Senior Communications Advisor
Issues management and media relations
Conseillère principale en communications
Gestion des enjeux et relations avec les médias
Public Safety Canada/Sécurité publique Canada
269 Laurier Avenue W/ 269, avenue Laurier ouest
Ottawa, (ON) K1P 0P8
(613) 944-4920
barbara.wilson@ps-sp.gc.ca

Hawrylak, Maciek

From: Kingsley, Michèle
Sent: October 27, 2011 12:35 PM
To: Filipps, Lisa
Cc: Paulson, Erika; Kwavnick, Andrea; Hawrylak, Maciek; MacDonald, Michael; Burton, Meredith; Wilson, Barbara; Slack, Jessica
Subject: FW: HEAD'S UP: CBC request re: privacy commissioner's letter

Hi Lisa,

Proposed Lines focusing on BSI that could have been used today:

- Today, basic subscriber information can be requested without a warrant under the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The proposed measures continue this practice but introduce accountability to the regime by adding robust recording, reporting, and audit requirements, none of which exist today.
- Our Government remains committed both to giving police the tools they need to do their job, and strongly protecting the privacy rights of Canadians.
- The proposed measures would fix the problem that occurs when the police and CSIS are unable to intercept communications because of a lack of intercept capable equipment at the service provider.
- The Courts will continue to review and authorize requests to intercept communications, except in exigent circumstances, as is the case today.

I note that the lines MO provided said "We are proposing measures", which suggests this is definitely coming forward - the same approach has been kept.

We will prepare a full package with categories of possible responses that could be pulled from in the future.

Thanks, m.

From: Filipps, Lisa
Sent: October 27, 2011 11:51 AM
To: Kingsley, Michèle; Paulson, Erika; Kwavnick, Andrea; Hawrylak, Maciek
Cc: MacDonald, Michael; Burton, Meredith; Wilson, Barbara; Slack, Jessica
Subject: Re: HEAD'S UP: CBC request re: privacy commissioner's letter

Thanks - we have a new call from the National Post and MO is receptive to getting some messages from you - Barb Wilson will be in touch.

From: Kingsley, Michèle
Sent: Thursday, October 27, 2011 11:45 AM
To: Filipps, Lisa; Paulson, Erika; Kwavnick, Andrea; Hawrylak, Maciek
Cc: MacDonald, Michael; Burton, Meredith; Wilson, Barbara; Slack, Jessica
Subject: RE: HEAD'S UP: CBC request re: privacy commissioner's letter

We will send you responsive lines that could have been used and could be used for future similar pieces.

From: Filipps, Lisa
Sent: October 27, 2011 11:15 AM
To: Kingsley, Michèle; Paulson, Erika; Kwavnick, Andrea; Hawrylak, Maciek

000224

24/11/2011

Cc: MacDonald, Michael; Burton, Meredith; Wilson, Barbara; Slack, Jessica
Subject: Re: HEAD'S UP: CBC request re: privacy commissioner's letter

I think that is likely closed for this call but I think our MO need some key points we could clarify for other calls. I would be happy to try to get some additional msgs up to them.

From: Kingsley, Michèle
Sent: Thursday, October 27, 2011 11:09 AM
To: Paulson, Erika; Kwavnick, Andrea; Hawrylak, Maciek
Cc: MacDonald, Michael; Burton, Meredith; Filippis, Lisa; Wilson, Barbara; Slack, Jessica
Subject: RE: HEAD'S UP: CBC request re: privacy commissioner's letter

Is there an opportunity to respond further? Or is the MO response pretty much it? Because we could respond directly to some points - such as her claim that we're lowering the threshold for BSI, which we're not... there are more... Do we have a window?

From: Paulson, Erika
Sent: October 27, 2011 11:02 AM
To: Kwavnick, Andrea; Hawrylak, Maciek
Cc: Kingsley, Michèle; MacDonald, Michael; Burton, Meredith; Filippis, Lisa; Wilson, Barbara; Slack, Jessica
Subject: HEAD'S UP: CBC request re: privacy commissioner's letter

Hi Andrea and Maciek,
Just a head's up that our issues management team received a request from CBC to respond to an open letter RE Lawful Access from the Privacy Commissioner to Minister Toews (please find link here: http://www.priv.gc.ca/media/nr-c/2011/let_111027_e.cfm#contenttop).

MO has responded with the following lines:

- As technology evolves, many criminal activities – such as the distribution of child pornography - become much easier.
- We are proposing measures to bring our laws into the 21st Century and provide police with the tools they need to do their job.
- Our approach strikes an appropriate balance between the investigative powers used to protect public safety and the necessity to safeguard the privacy of Canadians.

Also note: the Privacy Commissioner tweeted the letter in the last 15 minutes to over 3000 followers. We are already seeing retweets of it.

TWEET:

PrivacyPrivee Privacy Commission

#Privacy Commissioner outlines concerns about potential lawful access legislation. Letter to Minister of **@Safety** Canada <http://bit.ly/tqa78K>

Thanks,
Erika Paulson
613-993-4415

Reporter's Name

Media Outlet CBC Online

000225

24/11/2011

Call Date 10/27/2011 11:00 AM
Telephone
E-mail address @cbc.ca
Deadline 10/27/2011 5:00 PM
Status Consulting
Branch NS
Subject Lawful Access
Questions I was wondering if I could get a response from Minister Toews to Privacy Commissioner Jennifer Stoddart's letter about lawful access:

http://www.priv.gc.ca/media/nr-c/2011/let_111027_e.cfm#contenttop

I'm posting a story shortly and will add your response as soon as I receive it.

From: @CBC.CA]
Sent: Thursday, October 27, 2011 10:23:55 AM
To: PS Media Relations / Relations médias SP
Subject: CBC request re: privacy commissioner's letter
Auto forwarded by a Rule

Hi there,

I was wondering if I could get a response from Minister Toews to Privacy Commissioner Jennifer Stoddart's letter about lawful access:

http://www.priv.gc.ca/media/nr-c/2011/let_111027_e.cfm#contenttop

I'm posting a story shortly and will add your response as soon as I receive it.

Thanks so much,

CBCNews.ca
cbc.ca/technology
[@cbc.ca](mailto:)

Hawrylak, Maciek

From: Kingsley, Michèle
Sent: October 27, 2011 1:19 PM
To: Filipps, Lisa; Paulson, Erika; Kwavnick, Andrea; Hawrylak, Maciek
Cc: MacDonald, Michael; Burton, Meredith; Wilson, Barbara; Slack, Jessica; Swift, Andrew
Subject: RE: HEAD'S UP: CBC request re: privacy commissioner's letter

We got an official correspondence reply request with the OPC's letter.

Does Minister Toews have a twitter account? The PC tweeted her letter, so I would recommend tweeting our response back. If he does not, I would recommend posting the open response on the web and putting it out on the wires. Once it's ready we will work with you on that.

Thanks, Michèle

From: Filipps, Lisa
Sent: October 27, 2011 11:15 AM
To: Kingsley, Michèle; Paulson, Erika; Kwavnick, Andrea; Hawrylak, Maciek
Cc: MacDonald, Michael; Burton, Meredith; Wilson, Barbara; Slack, Jessica
Subject: Re: HEAD'S UP: CBC request re: privacy commissioner's letter

I think that is likely closed for this caal but I think our MO need some key points we could clarify for other calls. I would be happy to try to get some additional msgs up to them.

From: Kingsley, Michèle
Sent: Thursday, October 27, 2011 11:09 AM
To: Paulson, Erika; Kwavnick, Andrea; Hawrylak, Maciek
Cc: MacDonald, Michael; Burton, Meredith; Filipps, Lisa; Wilson, Barbara; Slack, Jessica
Subject: RE: HEAD'S UP: CBC request re: privacy commissioner's letter

Is there an opportunity to respond further? Or is the MO response pretty much it? Because we could respond directly to some points - such as her claim that we're lowering the threshold for BSI, which we're not... there are more... Do we have a window?

From: Paulson, Erika
Sent: October 27, 2011 11:02 AM
To: Kwavnick, Andrea; Hawrylak, Maciek
Cc: Kingsley, Michèle; MacDonald, Michael; Burton, Meredith; Filipps, Lisa; Wilson, Barbara; Slack, Jessica
Subject: HEAD'S UP: CBC request re: privacy commissioner's letter

Hi Andrea and Maciek,
Just a head's up that our issues management team received a request from CBC to respond to an open letter RE Lawful Access from the Privacy Commissioner to Minister Toews (please find link here: http://www.priv.gc.ca/media/nr-c/2011/let_111027_e.cfm#contenttop).

MO has responded with the following lines:

- As technology evolves, many criminal activities – such as the distribution of child pornography - become much easier.
- We are proposing measures to bring our laws into the 21st Century and provide police with the

000227

24/11/2011

tools they need to do their job.

- Our approach strikes an appropriate balance between the investigative powers used to protect public safety and the necessity to safeguard the privacy of Canadians.

Also note: the Privacy Commissioner tweeted the letter in the last 15 minutes to over 3000 followers. We are already seeing retweets of it.

TWEET:

PrivacyPrivee Privacy Commission

#Privacy Commissioner outlines concerns about potential lawful access legislation. Letter to Minister of @Safety Canada <http://bit.ly/tqa78K>

Thanks,
Erika Paulson
613-993-4415

Reporter's Name

Media Outlet CBC Online

Call Date 10/27/2011 11:00 AM

Telephone

E-mail address @cbc.ca

Deadline 10/27/2011 5:00 PM

Status Consulting

Branch NS

Subject Lawful Access

Questions I was wondering if I could get a response from Minister Toews to Privacy Commissioner Jennifer Stoddart's letter about lawful access:

http://www.priv.gc.ca/media/nr-c/2011/let_111027_e.cfm#contenttop

I'm posting a story shortly and will add your response as soon as I receive it.

From: @CBC.CA]
Sent: Thursday, October 27, 2011 10:23:55 AM
To: PS Media Relations / Relations médias SP
Subject: CBC request re: privacy commissioner's letter
Auto forwarded by a Rule

Hi there,

I was wondering if I could get a response from Minister Toews to Privacy Commissioner Jennifer Stoddart's

000228

24/11/2011

letter about lawful access:

http://www.priv.gc.ca/media/nr-c/2011/let_111027_e.cfm#contenttop

I'm posting a story shortly and will add your response as soon as I receive it.

Thanks so much,

CBCNews.ca
cbc.ca/technology
[@cbc.ca](#)

MacDonald, Michael

From: bmunson@itac.ca
Sent: October-27-11 5:14 PM
To: info@itac.ca
Subject: Privacy Commissioner outlines concerns about anticipated lawful-access legislation

ITAC Cyber Security Forum

FYI, here's the text of a letter from the Privacy Commissioner to the Minister of Public Safety outlining "her deep concerns about potential lawful access legislation." The related news release can be found at: http://www.priv.gc.ca/media/nr-c/2011/let_111027_e.cfm#contenttop

Bill Munson
ITAC

Letter to Minister of Public Safety Vic Toews

Privacy Commissioner of Canada Jennifer Stoddart has sent the following open letter to the Minister of Public Safety Vic Toews to outline her deep concerns about potential lawful access legislation.

October 26, 2011

Honourable Vic Toews, P.C., Q.C., M.P.
Minister of Public Safety
269 Laurier Avenue West
Ottawa, Ontario
K1A 0P8

Dear Minister Toews,

As you are aware, a growing number of questions are being raised – in Parliament, in legal circles and in the media – about potential lawful access legislation. I recognize that rapid developments in communication technologies are creating new challenges for law enforcement and national security authorities and that the Internet cannot be a lawless zone. However, in light of this recent public discussion, I feel it is important to set out once more my Office's own deep concerns prior to the reintroduction of legislation. This is why I have decided to write a letter to you, which I am making public.

My provincial and territorial privacy colleagues have also been seized by this issue and together we have called upon the federal government in 2009¹ and in 2012 to take a cautious approach to legislative proposals to create an expanded surveillance regime that would have serious repercussions for privacy rights. As your government prepares to bring forward legislation, I believe I have an obligation to outline my concerns about the potential impact on the privacy of Canadians.

Read together, the provisions of the lawful access bills from the last session of Parliament (C-50, C-51, and C-52) would have had a significant impact on our privacy rights. By expanding the legal tools of the state to conduct surveillance and access private information, and by reducing the depth of judicial scrutiny, the previous bills would have allowed government to subject more individuals to surveillance and scrutiny. In brief, these bills went far beyond simply

maintaining investigative capacity or modernizing search powers. Rather, they added significant new capabilities for investigators to track, and search and seize digital information about individuals.

Canadians expect their government to respect their fundamental rights and freedoms. Your government has made firm and repeated commitments to the importance of privacy. Consequently, when new surveillance powers are proposed in law, the burden of proof is with government to demonstrate the necessity, legal proportionality and practical effectiveness of these new powers. The government must also be prepared to demonstrate how the model it is proposing is the least privacy-invasive alternative possible.

Despite repeated calls, no systematic case has yet been made to justify the extent of the new investigative capabilities that would have been created by the bills. Canadian authorities have yet to provide the public with evidence to suggest that CSIS or Canadian police cannot perform their duties under the current regime. One-off cases and isolated incidents should not prove the rule, nor should exigent or emergency circumstances, for which there are already Criminal Code provisions.

As well, if the concern of law enforcement agencies is that it is difficult to obtain warrants or judicial authorization in a timely way, these administrative challenges should be addressed by administrative solutions rather than by weakening long-standing legal principles that uphold Canadians' fundamental freedoms.

I am also concerned about the adoption of lower thresholds for obtaining personal information from commercial enterprises. The new powers envisaged are not limited to specific, serious offences or urgent or exceptional situations. In the case of access to subscriber data, there is not even a requirement for the commission of a crime to justify access to personal information – real names, home address, unlisted numbers, email addresses, IP addresses and much more – without a warrant. Only prior court authorization provides the rigorous privacy protection Canadians expect.

In my view, the government has not convincingly demonstrated that there are no less privacy-invasive alternatives available to achieve its stated purpose.

Should Parliament ultimately opt to allow law enforcement and national security authorities to circumvent the courts to obtain personal information, we believe the oversight and reporting safeguards must be significantly strengthened.

The true importance of privacy protection is that it underpins our democratic freedoms. It allows us to exercise these freedoms openly, without fear, mistrust or censorship. This is why caution is so critical, to avoid the possible erosion of our free, open society.

To date, Canadians have not been given sufficient justification for the new powers when other, less intrusive alternatives could be explored. A focussed, tailored approach is vital.

As the government considers the reintroduction of the lawful access legislation I would respectfully ask that you take these comments into consideration.

Sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

c.c. Provincial and Territorial Privacy Commissioners Mr. William V. Baker, Deputy Minister, Public Safety

1 FPT 2009 Resolution

http://www.priv.gc.ca/media/nr-c/2009/res_090910_e.cfm (enclosed)

2 Letter to Mr. William Baker, March 9, 2011, http://www.priv.gc.ca/media/nr-c/2011/let_110309_e.cfm (enclosed)



Home > News Room > News

News Room

News

Select Year

Speeches

Select Year

Upcoming Events

Media Relations

Contact:

Anne-Marie Hayden
Tel: (613) 995-0103

Non-journalists are invited to contact our Information Centre. Please call 1-800-282-1376 (toll free) or (613) 947-1698 and ask to speak with an Information Officer.

Address:

112 Kent Street
Ottawa, ON
K1A 1H3
Fax: (613) 995-1139

News

Letter to Minister of Public Safety Vic Toews

Privacy Commissioner of Canada Jennifer Stoddart has sent the following open letter to the Minister of Public Safety Vic Toews to outline her deep concerns about potential lawful access legislation.

October 26, 2011

Honourable Vic Toews, P.C., Q.C., M.P.
Minister of Public Safety
269 Laurier Avenue West
Ottawa, Ontario
K1A 0P8

Dear Minister Toews,

As you are aware, a growing number of questions are being raised – in Parliament, in legal circles and in the media – about potential lawful access legislation. I recognize that rapid developments in communication technologies are creating new challenges for law enforcement and national security authorities and that the Internet cannot be a lawless zone. However, in light of this recent public discussion, I feel it is important to set out once more my Office's own deep concerns prior to the reintroduction of legislation. This is why I have decided to write a letter to you, which I am making public.

My provincial and territorial privacy colleagues have also been seized by this issue and together we have called upon the federal government in 2009¹ and in 2011² to take a cautious approach to legislative proposals to create an expanded surveillance regime that would have serious repercussions for privacy rights. As your government prepares

to bring forward legislation, I believe I have an obligation to outline my concerns about the potential impact on the privacy of Canadians.

Read together, the provisions of the lawful access bills from the last session of Parliament (C-50, C-51, and C-52) would have had a significant impact on our privacy rights. By expanding the legal tools of the state to conduct surveillance and access private information, and by reducing the depth of judicial scrutiny, the previous bills would have allowed government to subject more individuals to surveillance and scrutiny. In brief, these bills went far beyond simply maintaining investigative capacity or modernizing search powers. Rather, they added significant new capabilities for investigators to track, and search and seize digital information about individuals.

Canadians expect their government to respect their fundamental rights and freedoms. Your government has made firm and repeated commitments to the importance of privacy. Consequently, when new surveillance powers are proposed in law, the burden of proof is with government to demonstrate the necessity, legal proportionality and practical effectiveness of these new powers. The government must also be prepared to demonstrate how the model it is proposing is the least privacy-invasive alternative possible.

Despite repeated calls, no systematic case has yet been made to justify the extent of the new investigative capabilities that would have been created by the bills. Canadian authorities have yet to provide the public with evidence to suggest that CSIS or Canadian police cannot perform their duties under the current regime. One-off cases and isolated incidents should not prove the rule, nor should exigent or emergency circumstances, for which there are already *Criminal Code* provisions.

As well, if the concern of law enforcement agencies is that it is difficult to obtain warrants or judicial authorization in a timely way, these administrative challenges should be addressed by administrative solutions rather than by weakening long-standing legal principles that uphold Canadians' fundamental freedoms.

I am also concerned about the adoption of lower thresholds for obtaining personal information from commercial enterprises. The new powers envisaged are not limited to specific, serious offences or urgent or exceptional situations. In the case of access to subscriber data, there is not even a requirement for the commission of a crime to justify access to personal information – real names, home address, unlisted numbers, email addresses, IP addresses and much more – without a warrant. Only prior court authorization provides the rigorous privacy protection Canadians expect.

In my view, the government has not convincingly demonstrated that there are no less privacy-invasive alternatives available to achieve its stated purpose.

Should Parliament ultimately opt to allow law enforcement and national security authorities to circumvent the courts to obtain personal information, we believe the oversight and reporting safeguards must be significantly strengthened.

The true importance of privacy protection is that it underpins our democratic freedoms. It allows us to exercise these freedoms openly, without fear, mistrust or censorship. This is why caution is so critical, to avoid the possible erosion of our free, open society.

To date, Canadians have not been given sufficient justification for the new powers when other, less intrusive alternatives could be explored. A focussed, tailored approach is vital.

As the government considers the reintroduction of the lawful access legislation I would respectfully ask that you take these comments into consideration.

Sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

c.c. Provincial and Territorial Privacy Commissioners
Mr. William V. Baker, Deputy Minister, Public Safety

¹ FPT 2009 Resolution http://www.priv.gc.ca/media/nr-c/2009/res_090910_e.cfm
(enclosed)

² Letter to Mr. William Baker, March 9, 2011, http://www.priv.gc.ca/media/nr-c/2011/let_110309_e.cfm (enclosed)

Date Modified: 2011-10-27

MacDonald, Michael

From: Kingsley, Michèle
Sent: October-28-11 4:39 PM
To: MacDonald, Michael
Subject: Re: QP Transcript for October 28, 2011 / Transcription de la Période des questions pour le 28 octobre 2011

My pleasure. Matt Shogilev at DOJ was particularly helpful on this one and I forwarded your msg to him.

From: MacDonald, Michael
Sent: Friday, October 28, 2011 04:37 PM
To: Kingsley, Michèle
Subject: Fw: QP Transcript for October 28, 2011 / Transcription de la Période des questions pour le 28 octobre 2011

Thanks again.

From: Coburn, Stacey
Sent: Friday, October 28, 2011 04:36 PM
To: MacDonald, Michael
Subject: RE: QP Transcript for October 28, 2011 / Transcription de la Période des questions pour le 28 octobre 2011

Got it – so odd. I don't have the original anywhere (Lynda got it though). Anyway, thank you. The response has been provided up to the DM.

s

Stacey Coburn
949-4490

From: MacDonald, Michael
Sent: Friday, October 28, 2011 4:33 PM
To: Coburn, Stacey
Subject: Fw: QP Transcript for October 28, 2011 / Transcription de la Période des questions pour le 28 octobre 2011

Let me know if you get this. Thx

From: MacDonald, Michael
Sent: Friday, October 28, 2011 04:09 PM
To: Clairmont, Lynda; Coburn, Stacey
Cc: MacDonald, Michael; Kingsley, Michèle
Subject: Re: QP Transcript for October 28, 2011 / Transcription de la Période des questions pour le 28 octobre 2011

Lynda,

We worked with the team and DOJ on assessing this. Here's our assessment for passage to the DM.

Parts of the response are correct. The comments about authorities needing tools to address technological change and the bill having a balanced approach are helpful.

The comment that is problematic is the one stating that "No legislation proposed in the past, present or future by a conservative government would allow for police to read emails without a warrant". This is problematic because Section

184.4 of the criminal code currently provides for that. Furthermore, former C-50 would have enhanced the safeguards associated with s. 184.4 by adding notification and reporting requirements, without moving away from the authority to intercept in exceptional circumstances without judicial authorization. Therefore, given the Government was amending the provision to add safeguards to it, it can be inferred that the Government supports "warrantless interceptions". Note that former C-50 is a DOJ bill.

It may be of interest that this week we provided updated lines to Communications Branch on Lawful Access intended for the Minister's Office which would help to address some of these types of communications challenges.

Hope this helps.

From: Clairmont, Lynda
Sent: Friday, October 28, 2011 02:08 PM
To: MacDonald, Michael; Coburn, Stacey
Subject: Fw: QP Transcript for October 28, 2011 / Transcription de la Période des questions pour le 28 octobre 2011

Make it so pls

From: Baker, William V.
Sent: Friday, October 28, 2011 02:02 PM
To: Clairmont, Lynda
Subject: FW: QP Transcript for October 28, 2011 / Transcription de la Période des questions pour le 28 octobre 2011

Please review the Parliamentary Secretary's response to questions re: LA and warrants. Is this correct?

From: Leclair, Natalie **On Behalf Of** QP notes
Sent: October 28, 2011 1:32 PM
To: * EXCOM/COMEX; * Parliamentary Affairs Division / Division des affaires parlementaires; Alison Gregory; Allison, Catherine; Archambault-Chapleau, Nadine; Beaudoin, Serge C; Bendle, Victoria; Bernier, Melissa; Blackie, Ian; Bourdeau, Anne; Brock, Darlene; Burton, Meredith; Caroline Douglas; Charles-Eric.Lepine@rcmp-grc.gc.ca; Larose, Christine; Desnoyers, Christine; Clavel, Julien; Coburn, Stacey; COMDO; Cyr, Lynne; de Jager, Gabriela; Doré Charbonneau; Dupuis, Chantal; Duschner, Gabrielle; Dussault, Josée; Fournier, Muriel; Issues / Enjeux; Johnson, Mark; Koops, Randall; Lambert, Louise; Larose, Nathalie; Leclair, Natalie; Leclerc, Carole; LeSage, Lynn; Roylt; McAteer, Julie; Mcelhone, Kathryn; Paulson, Erika; Perry, Gates; Piasko, Ruba; Plunkett, Eva; priurma@npb-cnrc.gc.ca; Executive Services; Robin.Stong@cbsa-asfc.gc.ca; Ruth.Marier@cbsa-asfc.gc.ca; Scheewe, Nathan; Sellers, Philip; Shannon Muldoon; Stewart, Christena; Veilleux, Martine
Subject: QP Transcript for October 28, 2011 / Transcription de la Période des questions pour le 28 octobre 2011

Good afternoon,

Focus of Question Period today: Long-Gun Registry, Appointment of new Auditor General.

Questions answered by the Parliamentary Secretary today:

Françoise Boivin (Gatineau) asked a question regarding the Long-Gun Registry. (Transcript in)

>> The speaker: Order. Order. The honourable member for gatineau.

>> Mr. Speaker, the reckless and spiteful decision to destroy all gun registry records shows just how out of touch this government really is. Yesterday the quebec national assembly voted unanimously to demand the records be kept. They're even threatening legal action. Mr. Speaker, this government isn't just destroying records, it's destroying a key tool for keeping our communities safe. Why is this government insulting provinces that want to create their own registry? Why are they playing politics with public safety?

>> The speaker: The honorable parliamentary secretary to the minister of public safety.

>> Thank you, mr. Speaker. Our commitment to Canadians was to destroy and end the long gun registry. The long gun registry is the data. Mr. Speaker, the data is flawed. It's inaccurate. It doesn't target criminals. It targets law-abiding Canadians. Mr. Speaker, what we will continue is to have the licensing process that, information will be accessible to all law enforcement and to all agent circumstances but Mr. Speaker, make no mistakes we will end the long gun registry, which is the data. Thank you very much.

Earl Dreeshen (Red Deer) asked a question regarding the Long-Gun Registry. (Transcript in orange)

>> The speaker: The honourable member for red deer.

>> Mr. Speaker, Canadians gave our government a strong mandate to end the wasteful and ineffective long gun registry once and for all and that is exactly what we are doing. But Mr. Speaker members on this side of the house are not the only ones who received that mandate from the people of Canada. Many NDP M.P.s promised their constituents that if they sent them to this place, they would vote to end the long gun registry. However we've already seen many NDP members are breaking their promises to their constituents. Can the parliamentary secretary please tell the house how show views the decisions of these members opposite.

>> I want to thank the member from red deer for the good work he's done on helping us end the long gun registry. Mr. Speaker, I believe, I think we all believe that members must respect and represent the views of the Canadians who sent them here. I find it very disheartening to hear members say the fever has gone down a bit on gun registry in his riding or the member from western arctic who also campaigned on ending the long gun registry say he thinks it's appropriate for province to develop their own registry. Mr. Speaker, Canadians find this sort of hedging very unacceptable. When M.P.s make promises, Canadians expect those promises to be kept. And I call on all opposition members --

Dan Harris (Scarborough Southwest) asked a question regarding Lawful Access. (Transcript in red)

>> The speaker: The honourable member for Scarborough southwest.

>> Thank you, Mr. Speaker. This week the privacy commissioner sounded alarm bells again, raising serious concerns about the conservative government's lawful access legislation. The privacy commissioner said conservatives have not justified the sweeping search and seizure powers they plan to foist on commercial ISPs. Will the minister of public safety accept the privacy commissioner's recommendations and fix the legislation before it's reintroduced?

>> The speaker: The honourable parliamentary secretary to the minister of public safety.

>> Thank you, Mr. Speaker. Let me be perfectly clear: No legislation proposed in the past, present or future by a conservative government would allow for police to read emails without a warrant. As nothing evolves, many criminal activities such as the distribution of child pornography becomes more seizable and we are proposing measures to bring our laws into the 21st century. I do find it remarkable that the same party that wants to look at the private records of law-abiding gun owners was wanting to protect potential child pornographers. Thank you, Mr. Speaker.

>> The speaker: The honourable member for Scarborough southwest.

>> Well, Mr. Speaker, it was an answer but not one to my question. This is again about the privacy commissioner. The commissioner said this proposal will hugely respond surveillance and weaken judicial scrutiny we want far beyond what is needed. According to the commissioner better alternatives exist to give police the investigative tools they need while still preserving the privacy of Canadians. When will the government finally acknowledge these serious privacy concerns and agree to fix the bill?

>> The speaker: The honorable parliamentary secretary.

>> Our proposal will not allow for access to private communication without a warrant. What we are proposing is a balanced approach between checking on those who may be distributing child pornography and the rights of individuals to have their private information. Mr. Speaker, we ask on the NDP to support this good legislation, together with the 21st century, but also to support the private records of law-abiding long gun owners in this country. Thank you.

Peter Julian (Burnaby—New Westminster) asked a question regarding a compensation fund for firefighters. (Transcript in)

>> The speaker: The honourable member for burnaby-douglas.

>> Mr. Speaker, for 14 years canada's firefighters have been coming on parliament hill to ask that their families be taken care of if they die in the line of duty, if they die saving others through a public safety officer compensation fund. Now, five years ago, mr. Speaker, the ndp delivered, then we passed legislation through the house directing the government to do this. Since that time dozens of canada's firefighters and police officers have passed away and their families are often left destute. The united states has a fund. Canada doesn'T. Why won't the government establish a public safety officer compensation fund and why are they showing such profound disrespect to canada's firefighters and police officers?

>> The speaker: The honorable parliamentary secretary to the minister of public safety.

>> Thank you, mr. Speaker. Mr. Speaker, this is the government that is listening to firefighters and police officers across the country. That's why we are giving them the tools they need to do their job. That's why we introduced a volunteer tax credit, mr. Speaker, which has been supported across the country. It's something fire fighters asked for. It's helping them. We respect and appreciate the work that they do. We'll continue to support them. We ask the option to do -- ask the toption do the same thing, vote for measures that will keep criminals in jail and not on the street. Thank you.

Note:

Massimo Pacetti (Saint-Léonard—Saint-Michel) asked a question regarding the Long-Gun Registry. The Leader of the Government in the House of Commons responded. (Transcript in **blue**)

Françoise Boivin (Gatineau) asked a question regarding the Long-Gun Registry. The Minister of State (Small Business and Tourism) responded. (Transcript in **green**)

Rosane Doré Lefebvre (Alfred—Pelan) asked a question regarding the Long-Gun Registry. The Minister of State (Small Business and Tourism) responded. (Transcript in **purple**)

The English unofficial transcript is attached.

Thank you

Bon après-midi,

Focus de la Période des questions aujourd'hui : Le registre des armes d'épaules, la nomination du nouveau vérificateur général.

La secrétaire parlementaire a répondu aux questions qui suivent :

Françoise Boivin (Gatineau) a posé une question concernant le registre des armes d'épaule. (Transcription en)

Earl Dreeshen (Red Deer) a posé une question concernant le registre des armes d'épaule. (Transcription en orange)

Dan Harris (Scarborough-Sud-Ouest) a posé une question concernant l'accès légal. (Transcription en rouge)

Peter Julian (Burnaby—New Westminster) a posé une question concernant un fonds d'indemnisation pour les pompiers. (Transcription en)

Notez :

Massimo Pacetti (Saint-Léonard—Saint-Michel) a posé une question concernant le registre des armes d'épaule. Le Leader du gouvernement à la Chambre des communes a répondu. (Transcription en **bleu**)

Françoise Boivin (Gatineau) a posé une question concernant le registre des armes d'épaule. Le ministre d'État (Petite Entreprise et Tourisme) a répondu. (Transcription en vert)

Rosane Doré Lefebvre (Alfred—Pelan) a posé une question concernant le registre des armes d'épaule. Le ministre d'État (Petite Entreprise et Tourisme) a répondu. (Transcription en **mauve**)

Veillez prendre note que la transcription n'est disponible qu'en anglais seulement. La transcription sera offerte dans les deux langues officielles demain matin sur le site www.parl.gc.ca. Merci de votre compréhension.

Natalie Leclair

Advisor / Conseillère

Parliamentary Affairs / Affaires parlementaires

Public Safety Canada / Sécurité publique Canada

Tel/Tél: (613) 990-2718

Fax: (613) 954-8774

Email/Courriel: natalie.leclair@ps-sp.gc.ca

BASIC SUBSCRIBER INFORMATION

Critics of proposed lawful access legislation have expressed concern that the provision of basic subscriber information to authorities upon request, and to police in emergencies, interferes with citizen's expectation of privacy.

In 2007, Public Safety Canada held public consultations regarding these provisions specifically, in which the Office of the Privacy Commissioner of Canada (OPC) participated. They noted that all basic subscriber information is considered personal information.

At this time, the OPC maintained that there is a reasonable expectation of privacy for certain, "confidential" customer information. For example, they consider unlisted telephone numbers to be confidential, as individuals have gone through the process of having their names removed, and having paid for this removal, it can be assumed that they consider this information private.

The OPC noted that this same expectation of privacy also applies to wireless cell phone numbers, and individuals typically only share these numbers with their friends and family. They also felt that the users of the Internet expect privacy, as many use pseudonyms to communicate and participate in activities online anonymously. They categorize this type of information as confidential.

On the other hand, OPC has demonstrated that some of the basic subscriber information, namely **customer name, address and listed telephone number, is considered non-confidential**. In 2009, the Canadian Radio-television and Telecommunications Commission (CRTC) consulted on whether telecommunications service providers (TSPs) could share customer information with a TSP company affiliated to the customer's TSP (for example, if a phone provider and an internet provider are owned by the same company but are operated separately as affiliates, the phone company may want to provide the customer data to their internet affiliate)¹. In this context, the OPC reiterated that customer name, address and listed phone number are not considered confidential and are exempt from consent requirements, but emphasized that express consent from the customer should always be maintained any time that other information is shared.

Consent is relevant to the work we are doing today because many court cases look at the user agreements between TSPs and their customers to determine if there is a reasonable expectation of privacy. The need for express consent to share personal information was made in a 2003 CRTC decision², in which the CRTC compelled TSPs to modify their customer contracts to ensure that express consent by the customer to share their personal information was incorporated. One particular reference made by the CRTC was that unless express consent is obtained to do so, all information kept by the company regarding the customer, **other than the customer's name, address and listed telephone number**, is confidential and may not be disclosed by the company. There are exceptions

¹ CRTC Telecom Decision 2009-723

² CRTC Telecom Decision 2003-33-1

to this, including if the disclosure is pursuant to a legal power. It is assumed that this refers to a warrant or subpoena in particular.

In various decisions, the CRTC itself has made the distinction between confidential and non-confidential customer information related specifically to wireline telephony. In 2001, a CRTC Order³ approved a tariff for Bell Canada's Local Service Provider Identification (LSPID) service to law enforcement agencies in respect of published wireline numbers, as they concluded that this information does not provide information about a person's lifestyle and therefore privacy is not affected. Of note is that the name associated to the LSPID would not be released.

The CRTC has acknowledged that the provision of non-confidential name, address and listed telephone number to requesting law enforcement without a warrant is an important and efficient tool for investigations⁴. In a 2000 Telecom Order⁵, the CRTC ruled that it does not have jurisdiction over tariffs associated with the provision of confidential customer information to law enforcement pursuant to court orders (i.e. warrants and assistance orders).

Legal Opinion

**Pages 243 to / à 246
are withheld pursuant to section
sont retenues en vertu de l'article**

**of the Access to Information
de la Loi sur l'accès à l'information**

Kingsley, Michèle

From: Kingsley, Michèle
Sent: October 31, 2011 12:21 PM
To: Kwavnick, Andrea; Hawrylak, Maciek; Kousha, Hasti; Scott, Marcie; Audcent, Karen
Subject: ARTICLE: Privacy invasion shouldn't be 'lawful'

Privacy invasion shouldn't be 'lawful'

Ann Cavoukian, National Post · Oct. 31, 2011 | Last Updated: Oct. 31, 2011 4:07 AM ET

I must add my voice to the growing dismay regarding the impact of impending "lawful access" legislation in this country. In my view, it is highly misleading to call it "lawful." Let's call it what it is - a system of expanded surveillance.

At issue is the anticipated re-introduction of a trio of federal bills that will provide police with much greater ability to access and track information, via the communications technologies we use every day, such as the Internet, smart phones and other mobile devices. I have no doubt that, collectively, the legislation will substantially diminish the privacy rights of Ontarians and Canadians as a whole.

Let's take a brief look at the surveillance bills, which were introduced prior to the last election:

? Bill C-50 would make it easier for the police to obtain judicial approval of multiple intercept and tracking warrants and production orders, to access and track e-communications.

? Bill C-51 would give the police new powers to obtain court orders for remote live tracking, as well as suspicion-based orders requiring telecommunication service providers and other companies to preserve and turn over data of interest to the police.

? Bill C-52 would require telecommunication service providers to build and maintain intercept capability into their networks for use by law enforcement, and gives the police warrantless power to access subscriber information.

I well understand the attraction for law enforcement officials - the increased ability to access and track our e-communications, with reduced judicial scrutiny, would put a treasure trove of new information at their fingertips.

However, we must be extremely careful not to allow the admitted investigative needs of police forces to interfere with or violate our constitutional right to be secure from unreasonable state surveillance. The proposed surveillance powers come at the expense of the necessary privacy safeguards guaranteed under the Charter of Rights and Freedoms. The federal government must be persuaded to acknowledge the sensitivity of traffic data, stored data and tracking data, and strongly urged to re-draft the bills. For a start, the proposal for warrantless access to subscriber information is untenable and should be withdrawn. If special access to subscriber information is considered to be absolutely necessary, it must take place under a court-supervised regime.

The government needs to step back and consider all of these implications. A comprehensive

cost-benefit analysis should precede the entrenchment of so many significant public policy decisions. Public Parliamentary hearings must also be scheduled to ensure that civil society, as well as the telecom industry, has a full opportunity to provide input.

Canadians must press the federal government to publicly commit to enacting muchneeded oversight legislation in tandem with any expansive surveillance measures. Intrusive proposals require, at the very least, matching legislative safeguards. The courts, affected individuals, future Parliaments and the public must be well informed about the scope, effectiveness and damaging negative effects of such intrusive powers.

We can, and must, have both greater security and privacy, in unison. It cannot be one at the expense of the other. The true value of privacy must be recognized in any effort to modernize law enforcement powers. Imposing a mandatory surveillance regime on the public and its telecom service providers must not go forward without strong safeguards to protect the future of our fundamental freedoms.

- Ann Cavoukian is the Information Privacy Commissioner of Ontario.

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

**Pages 249 to / à 251
are duplicates of
sont des duplicatas des
pages 260 to / à 262**

Kingsley, Michèle

From: bmunson@itac.ca
Sent: October 27, 2011 5:14 PM
To: info@itac.ca
Subject: Privacy Commissioner outlines concerns about anticipated lawful-access legislation

ITAC Cyber Security Forum

FYI, here's the text of a letter from the Privacy Commissioner to the Minister of Public Safety outlining "her deep concerns about potential lawful access legislation." The related news release can be found at:
http://www.priv.gc.ca/media/nr-c/2011/let_111027_e.cfm#contenttop

Bill Munson
ITAC

Letter to Minister of Public Safety Vic Toews

Privacy Commissioner of Canada Jennifer Stoddart has sent the following open letter to the Minister of Public Safety Vic Toews to outline her deep concerns about potential lawful access legislation.

October 26, 2011

Honourable Vic Toews, P.C., Q.C., M.P.
Minister of Public Safety
269 Laurier Avenue West
Ottawa, Ontario
K1A 0P8

Dear Minister Toews,

As you are aware, a growing number of questions are being raised - in Parliament, in legal circles and in the media - about potential lawful access legislation. I recognize that rapid developments in communication technologies are creating new challenges for law enforcement and national security authorities and that the Internet cannot be a lawless zone. However, in light of this recent public discussion, I feel it is important to set out once more my Office's own deep concerns prior to the reintroduction of legislation. This is why I have decided to write a letter to you, which I am making public.

My provincial and territorial privacy colleagues have also been seized by this issue and together we have called upon the federal government in 2009 and in 2012 to take a cautious approach to legislative proposals to create an expanded surveillance regime that would have serious repercussions for privacy rights. As your government prepares to bring forward legislation, I believe I have an obligation to outline my concerns about the potential impact on the privacy of Canadians.

Read together, the provisions of the lawful access bills from the last session of Parliament (C-50, C-51, and C-52) would have had a significant impact on our privacy rights. By expanding the legal tools of the state to conduct surveillance and access private information, and by reducing the depth of judicial scrutiny, the previous bills would have allowed government to subject more individuals to surveillance and scrutiny. In brief, these bills went far beyond simply maintaining investigative capacity or modernizing search powers. Rather, they added significant new capabilities for investigators to track, and search and seize digital information about individuals.

Canadians expect their government to respect their fundamental rights and freedoms. Your government has made firm and repeated commitments to the importance of privacy. Consequently, when new surveillance powers are proposed in law, the burden of proof is with government to demonstrate the necessity, legal proportionality and practical effectiveness of these new powers. The government must also be prepared to demonstrate

how the model it is proposing is the least privacy-invasive alternative possible.

Despite repeated calls, no systematic case has yet been made to justify the extent of the new investigative capabilities that would have been created by the bills. Canadian authorities have yet to provide the public with evidence to suggest that CSIS or Canadian police cannot perform their duties under the current regime. One-off cases and isolated incidents should not prove the rule, nor should exigent or emergency circumstances, for which there are already Criminal Code provisions.

As well, if the concern of law enforcement agencies is that it is difficult to obtain warrants or judicial authorization in a timely way, these administrative challenges should be addressed by administrative solutions rather than by weakening long-standing legal principles that uphold Canadians' fundamental freedoms.

I am also concerned about the adoption of lower thresholds for obtaining personal information from commercial enterprises. The new powers envisaged are not limited to specific, serious offences or urgent or exceptional situations. In the case of access to subscriber data, there is not even a requirement for the commission of a crime to justify access to personal information - real names, home address, unlisted numbers, email addresses, IP addresses and much more - without a warrant. Only prior court authorization provides the rigorous privacy protection Canadians expect.

In my view, the government has not convincingly demonstrated that there are no less privacy-invasive alternatives available to achieve its stated purpose.

Should Parliament ultimately opt to allow law enforcement and national security authorities to circumvent the courts to obtain personal information, we believe the oversight and reporting safeguards must be significantly strengthened.

The true importance of privacy protection is that it underpins our democratic freedoms. It allows us to exercise these freedoms openly, without fear, mistrust or censorship. This is why caution is so critical, to avoid the possible erosion of our free, open society.

To date, Canadians have not been given sufficient justification for the new powers when other, less intrusive alternatives could be explored. A focussed, tailored approach is vital.

As the government considers the reintroduction of the lawful access legislation I would respectfully ask that you take these comments into consideration.

Sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

c.c. Provincial and Territorial Privacy Commissioners Mr. William V. Baker, Deputy
Minister, Public Safety

1 FPT 2009 Resolution
http://www.priv.gc.ca/media/nr-c/2009/res_090910_e.cfm (enclosed)

2 Letter to Mr. William Baker, March 9, 2011, http://www.priv.gc.ca/media/nr-c/2011/let_110309_e.cfm (enclosed)

**Pages 254 to / à 257
are duplicates of
sont des duplicatas des
pages 265 to / à 268**

**Pages 258 to / à 259
are duplicates of
sont des duplicatas des
pages 247 to / à 248**

Scott, Marcie

From: Kwavnick, Andrea
Sent: October 31, 2011 4:31 PM
To: Scott, Marcie; Durand, Mathieu
Subject: FW: URGENT OPC meeting
Attachments: Privacy Commissioner outlines concerns about anticipated lawful-access legislation; CNA Examples for PS (2011-10-28)_1.doc; CNA Numbers - RCMP (2011-10-25)_1.doc

FYI

From: Kingsley, Michèle
Sent: October 31, 2011 10:55 AM
To: Kwavnick, Andrea; Hawrylak, Maciek
Subject: FW: URGENT OPC meeting

From: Yves Desjardins [mailto:Yves.Desjardins@rcmp-grc.gc.ca]
Sent: October 31, 2011 10:56 AM
To: Kingsley, Michèle
Subject: Fwd: URGENT OPC meeting

Good morning Michele,

Attached are CNA examples as promised. As well, I include some data for un-warranted CNA requests.

Yves

J.R.Yves DESJARDINS, Insp.
Royal Canadian Mounted Police
Technical Operations
OIC Special 'I' Branch
2300D - 1426 St-Joseph Blvd.
Ottawa, ON - Canada
K1A 0R2

Tel. #: +1 (613) 990-1353
Mobile: +1 (613) 882-1353
Blackberry PIN: 231AA0FE
email: yves.desjardins@rcmp-grc.gc.ca
>>> Stan Burke 2011/10/28 12:15 PM >>>
Good afternoon,

This is further to your email of 2011-09-23 13:40 hrs RE: Comms lines

You requested to see the final product prior to its release - please reference CNA Examples for PS below. We are still in the process of obtaining further information to refine other examples. Please

000260

25/11/2011

refer to attached documents and advise us whether you concur with its release.

Thank you.

Stan

Stan Burke, Chief Superintendent / Surintendant principal
Royal Canadian Mounted Police / Gendarmerie royale du Canada
Director General
Technical Investigation Services / Directeur général des services d'enquête techniques
1426 St. Joseph Blvd., Room / pièce 2300A
Ottawa, Ontario K1A 0R2
Phone# /Tél: (613) 993-2986
Cell#:(613): (613) 883-8733
Fax#/Télec: (613) 993-6872
e-mail/courriel: Stan.Burke@rcmp-grc.gc.ca

This electronic mail message is intended only for the use of the party(ies) to whom it is addressed. This message may contain information that is privileged or confidential. Any use of the information by anyone other than the intended recipient(s) is prohibited. If you receive this message in error, please notify the sender immediately and delete both the original message and all copies. Thank you.

Ce courrier électronique est réservé à l'usage des personnes auxquelles il s'adresse. Ce message peut contenir de l'information protégée ou confidentielle. Toute utilisation de l'information par des personnes autres que celles auxquelles il s'adresse est interdite. Si vous avez reçu ce message par erreur, veuillez en aviser immédiatement l'expéditeur et détruisez le message original ainsi que les copies. Merci.

>>>

From: Yves Desjardins
To: Burke, Stan
Date: 2011-10-28 10:30 AM
Subject: Fwd: URGENT OPC meeting

Good morning Sir,

Further to yesterday public release of the Privacy Commissioner's letter to Vic Toews, Minister of Public Safety, regarding un-warranted access to CNA information, I received this urgent request from Michele Kingsley, PS National Security Operations, would like to get the examples as soon as possible to brief Minister Toews and prepare a reply to the Privacy Commissioner.

Attached are seven (7) examples where un-warranted access to CNA information helped/hampered police investigation. I request RCMP's approval to release these examples to Public Safety to be used. It is likely these examples will be made public.

J.R.Yves DESJARDINS, Insp.
Royal Canadian Mounted Police
Technical Operations
OIC Special 'I' Branch

000261

25/11/2011

2300D - 1426 St-Joseph Blvd.
Ottawa, ON - Canada
K1A 0R2

Tel. #: +1 (613) 990-1353

Mobile: +1 (613) 882-1353

Blackberry PIN: 231AA0FE

email: yves.desjardins@rcmp-grc.gc.ca

>>> Kingsley, Michèle<Michele.Kingsley@ps-sp.gc.ca> 2011/10/27 11:38 AM >>>

Yves, Mark, Mollie,

We are going to be meeting with the Office of the Privacy Commissioner next week. If you've seen the open letter she tweeted to Minister Toews this morning you know that she is, again, calling for a demonstration of a convincing need by law enforcement agencies for BSI.

So to follow up on our request of last month, we now URGENTLY need these examples and any supporting stats/data.

Thanks, 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

Scott, Marcie

From: bmunson@itac.ca
Sent: October 27, 2011 5:14 PM
To: info@itac.ca
Subject: Privacy Commissioner outlines concerns about anticipated lawful-access legislation

ITAC Cyber Security Forum

FYI, here's the text of a letter from the Privacy Commissioner to the Minister of Public Safety outlining "her deep concerns about potential lawful access legislation." The related news release can be found at:
http://www.priv.gc.ca/media/nr-c/2011/let_111027_e.cfm#contenttop

Bill Munson
ITAC

Letter to Minister of Public Safety Vic Toews

Privacy Commissioner of Canada Jennifer Stoddart has sent the following open letter to the Minister of Public Safety Vic Toews to outline her deep concerns about potential lawful access legislation.

October 26, 2011

Honourable Vic Toews, P.C., Q.C., M.P.
Minister of Public Safety
269 Laurier Avenue West
Ottawa, Ontario
K1A 0P8

Dear Minister Toews,

As you are aware, a growing number of questions are being raised - in Parliament, in legal circles and in the media - about potential lawful access legislation. I recognize that rapid developments in communication technologies are creating new challenges for law enforcement and national security authorities and that the Internet cannot be a lawless zone. However, in light of this recent public discussion, I feel it is important to set out once more my Office's own deep concerns prior to the reintroduction of legislation. This is why I have decided to write a letter to you, which I am making public.

My provincial and territorial privacy colleagues have also been seized by this issue and together we have called upon the federal government in 2009¹ and in 2011² to take a cautious approach to legislative proposals to create an expanded surveillance regime that would have serious repercussions for privacy rights. As your government prepares to bring forward legislation, I believe I have an obligation to outline my concerns about the potential impact on the privacy of Canadians.

Read together, the provisions of the lawful access bills from the last session of Parliament (C-50, C-51, and C-52) would have had a significant impact on our privacy rights. By expanding the legal tools of the state to conduct surveillance and access private information, and by reducing the depth of judicial scrutiny, the previous bills would have allowed government to subject more individuals to surveillance and scrutiny. In brief, these bills went far beyond simply maintaining investigative capacity or modernizing search powers. Rather, they added significant new capabilities for investigators to track, and search and seize digital information about individuals.

Canadians expect their government to respect their fundamental rights and freedoms. Your government has made firm and repeated commitments to the importance of privacy. Consequently, when new surveillance powers are proposed in law, the burden of proof is with government to demonstrate the necessity, legal proportionality and practical effectiveness of these new powers. The government must also be prepared to demonstrate

how the model it is proposing is the least privacy-invasive alternative possible.

Despite repeated calls, no systematic case has yet been made to justify the extent of the new investigative capabilities that would have been created by the bills. Canadian authorities have yet to provide the public with evidence to suggest that CSIS or Canadian police cannot perform their duties under the current regime. One-off cases and isolated incidents should not prove the rule, nor should exigent or emergency circumstances, for which there are already Criminal Code provisions.

As well, if the concern of law enforcement agencies is that it is difficult to obtain warrants or judicial authorization in a timely way, these administrative challenges should be addressed by administrative solutions rather than by weakening long-standing legal principles that uphold Canadians' fundamental freedoms.

I am also concerned about the adoption of lower thresholds for obtaining personal information from commercial enterprises. The new powers envisaged are not limited to specific, serious offences or urgent or exceptional situations. In the case of access to subscriber data, there is not even a requirement for the commission of a crime to justify access to personal information - real names, home address, unlisted numbers, email addresses, IP addresses and much more - without a warrant. Only prior court authorization provides the rigorous privacy protection Canadians expect.

In my view, the government has not convincingly demonstrated that there are no less privacy-invasive alternatives available to achieve its stated purpose.

Should Parliament ultimately opt to allow law enforcement and national security authorities to circumvent the courts to obtain personal information, we believe the oversight and reporting safeguards must be significantly strengthened.

The true importance of privacy protection is that it underpins our democratic freedoms. It allows us to exercise these freedoms openly, without fear, mistrust or censorship. This is why caution is so critical, to avoid the possible erosion of our free, open society.

To date, Canadians have not been given sufficient justification for the new powers when other, less intrusive alternatives could be explored. A focussed, tailored approach is vital.

As the government considers the reintroduction of the lawful access legislation I would respectfully ask that you take these comments into consideration.

Sincerely,

Original signed by

Jennifer Stoddart
Privacy Commissioner of Canada

c.c. Provincial and Territorial Privacy Commissioners Mr. William V. Baker, Deputy
Minister, Public Safety

1 FPT 2009 Resolution
http://www.priv.gc.ca/media/nr-c/2009/res_090910_e.cfm (enclosed)

2 Letter to Mr. William Baker, March 9, 2011, http://www.priv.gc.ca/media/nr-c/2011/let_110309_e.cfm (enclosed)

Sgt. Bernard Tremblay
October 28, 2011

Police "CNA Request" Examples for Public Safety

Sgt. Bernard Tremblay
October 28, 2011

- 6 The National Child Exploitation Coordination Centre forwarded packages to police across Canada for *Operation Carole*: **access to child porn sites** by people from different countries (investigation originating from Luxembourg). As the images sent out to investigators do not meet the *Criminal Code* definition of child pornography, Production Orders or Search Warrants could not be obtained.

Since the TSPs in Atlantic Canada did not provide subscriber information without a court order, Nova Scotia investigators had no way of determining who the suspects were and had to conclude their investigations.

(Source: Halifax RCMP – Integrated ICE Unit)

- 7 In Spring 2011, during an investigation of peer-to-peer **sharing of child pornography**, New Brunswick RCMP identified 130 IP addresses which they believed to be associated to the same suspect.

(Source: New Brunswick RCMP - ICE Unit)

Basic Subscriber Information (CNA) 2010

1. Form 6306¹

RCMP

- Number of CNA requests reported by RCMP in 2010: 28 143
 - CNA provided voluntarily by TSP: 26 331 (93.6%)
 - CNA not provided. TSP refused to cooperate without a court order: 1 812 (6.4%)

2. Law Enforcement Requests (LERs)²

National Child Exploitation Coordination Centre (NCECCC)

- Number of LERs sent to TSPs: 1 244
 - CNA provided voluntarily by TSP: 902 (72.5%)
 - CNA not provided by TSP: 342 (27.5%)
 - TSP refused to cooperate: 62 (5%)
 - TSP did not reply: 53 (4.3%)
 - Data not available: 227 (18.2%)
- Average LER response time: 13 days

¹ Although this data provides some information about CNA requests by Canadian law enforcement agencies (LEAs), it is not complete as the RCMP reporting tool was not consistently used by RCMP Units and other LEAs. Also, when a TSP is known to refuse to cooperate without a court order, investigators, if they have sufficient grounds to do so, will often apply for a court order without first requesting voluntary disclosure from the TSP. This is not always reported.

² NCECC (Ottawa) data is from LERs and is not included in the data from Form 6306.

Sgt. Bernard Tremblay
October 25, 2011

Page 269
is a duplicate of
est un duplicata de la
page 281

**Pages 270 to / à 271
are duplicates of
sont des duplicatas des
pages 280 to / à 281**

**Pages 272 to / à 273
are duplicates of
sont des duplicatas des
pages 280 to / à 281**

**Pages 274 to / à 275
are duplicates of
sont des duplicatas des
pages 278 to / à 279**

**Pages 276 to / à 277
are duplicates of
sont des duplicatas des
pages 280 to / à 281**

Kingsley, Michèle

From: Kingsley, Michèle
Sent: October 31, 2011 5:04 PM
To: Filipps, Lisa; MacDonald, Michael
Cc: Paulson, Erika; Burton, Meredith; Kwavnick, Andrea; Hawrylak, Maciek
Subject: RE: FOR REVIEW: Letter to the Editor - National Post
Our emails crossed - there is a line in there that is problematic...

From: Filipps, Lisa
Sent: October 31, 2011 5:02 PM
To: Kingsley, Michèle; MacDonald, Michael
Cc: Paulson, Erika; Burton, Meredith; Kwavnick, Andrea; Hawrylak, Maciek
Subject: RE: FOR REVIEW: Letter to the Editor - National Post

Hi Michele –

Unfortunately it seems that MO has already submitted. I'm very sorry as I was under the impression there would be an opportunity to comment.

From: Kingsley, Michèle
Sent: Monday, October 31, 2011 4:47 PM
To: Filipps, Lisa; MacDonald, Michael
Cc: Paulson, Erika; Burton, Meredith; Kwavnick, Andrea; Hawrylak, Maciek
Subject: RE: FOR REVIEW: Letter to the Editor - National Post

Hi Lisa,

Thanks for the opportunity to respond. What's the deadline?

Thanks, Michèle

From: Filipps, Lisa
Sent: October 31, 2011 4:34 PM
To: MacDonald, Michael; Kingsley, Michèle
Cc: Paulson, Erika; Burton, Meredith
Subject: FOR REVIEW: Letter to the Editor - National Post

Mike and Michele –

The Minister's Office provided us with a Letter to the Editor they will be sending for publication on Wednesday. Could you please review and flag any factual errors? Please note that we are asking for a disaster check only. Thank you!

I read with interest Ontario Privacy Commissioner Ann Cavoukian's opinion piece on Monday, October 31st regarding our Government's proposed lawful access legislation. I would like to clear up some clear inaccuracies.

By moving quickly to reintroduce comprehensive law-and-order legislation, our Government is fulfilling our commitment to take action to protect families and hold criminals accountable.

Lawful access legislation will continue that theme. Technology is a critical aspect of the way Canadians do business and communicate with each other. However, as technology advances, many criminal activities become easier. In the face of this reality, we will be proposing legislation that strikes an appropriate balance between the privacy rights of Canadians and the ability of police to enforce our laws.

There are two components to our lawful access proposals. First, we will allow police officers to access “phone book” information from telecom service providers. While carrying out an investigation if it becomes necessary to find a suspect’s name, address, phone number, or other similar identifier, companies will be required to disclose that information. Second, telecom providers will be required to have the capacity to allow for police officers to investigate, with a warrant, all communications methods.

Let me be clear. No legislation proposed in the past, present, or future by a Conservative Government will create powers for police to read emails without a warrant. Our proposed approach of linking an internet address to subscriber information is on par with the phone book linking phone numbers to an address. What this will NOT allow for is access to private communications without a warrant.

That being said, our message is clear: if you use technology to commit crimes – like distributing child pornography – the police will apprehend you and you will be punished to the fullest extent of the law.

Vic Toews
Minister of Public Safety

Hawrylak, Maciek

From: Filipps, Lisa
Sent: October 31, 2011 6:11 PM
To: Kingsley, Michèle; MacDonald, Michael
Cc: Paulson, Erika; Burton, Meredith; Kwavnick, Andrea; Hawrylak, Maciek
Subject: Re: FOR REVIEW: Letter to the Editor - National Post

Michele - I shared you comment with the MO.

From: Kingsley, Michèle
Sent: Monday, October 31, 2011 05:03 PM
To: Filipps, Lisa; MacDonald, Michael
Cc: Paulson, Erika; Burton, Meredith; Kwavnick, Andrea; Hawrylak, Maciek
Subject: RE: FOR REVIEW: Letter to the Editor - National Post

Thanks. I can tell you right now that the sentence stating that "No legislation proposed in the past, present or future by a conservative government would allow for police to read emails without a warrant" is problematic because Section 184.4 of the criminal code currently provides for that. Furthermore, former C-50 would have enhanced the safeguards associated with s. 184.4 by adding notification and reporting requirements, without moving away from the authority to intercept in exceptional circumstances without judicial authorization. Therefore, given the Government was amending the provision to add safeguards to it, it can be inferred that the Government supports "warrantless interceptions". Note that former C-50 is a DOJ bill.

From: Filipps, Lisa
Sent: October 31, 2011 5:01 PM
To: Kingsley, Michèle; MacDonald, Michael
Cc: Paulson, Erika; Burton, Meredith; Kwavnick, Andrea; Hawrylak, Maciek
Subject: RE: FOR REVIEW: Letter to the Editor - National Post

I'm waiting for a response and will let you know as soon as I hear.

From: Kingsley, Michèle
Sent: Monday, October 31, 2011 4:47 PM
To: Filipps, Lisa; MacDonald, Michael
Cc: Paulson, Erika; Burton, Meredith; Kwavnick, Andrea; Hawrylak, Maciek
Subject: RE: FOR REVIEW: Letter to the Editor - National Post

Hi Lisa,

Thanks for the opportunity to respond. What's the deadline?

Thanks, Michèle

From: Filipps, Lisa
Sent: October 31, 2011 4:34 PM
To: MacDonald, Michael; Kingsley, Michèle
Cc: Paulson, Erika; Burton, Meredith
Subject: FOR REVIEW: Letter to the Editor - National Post

000280

24/11/2011

Mike and Michele

The Minister's Office provided us with a Letter to the Editor they will be sending for publication on Wednesday. Could you please review and flag any factual errors? Please note that we are asking for a disaster check only. Thank you!

I read with interest Ontario Privacy Commissioner Ann Cavoukian's opinion piece on Monday, October 31st regarding our Government's proposed lawful access legislation. I would like to clear up some clear inaccuracies.

By moving quickly to reintroduce comprehensive law-and-order legislation, our Government is fulfilling our commitment to take action to protect families and hold criminals accountable.

Lawful access legislation will continue that theme. Technology is a critical aspect of the way Canadians do business and communicate with each other. However, as technology advances, many criminal activities become easier. In the face of this reality, we will be proposing legislation that strikes an appropriate balance between the privacy rights of Canadians and the ability of police to enforce our laws.

There are two components to our lawful access proposals. First, we will allow police officers to access phone book information from telecom service providers. While carrying out an investigation if it becomes necessary to find a suspect's name, address, phone number, or other similar identifier, companies will be required to disclose that information. Second, telecom providers will be required to have the capacity to allow for police officers to investigate, with a warrant, all communications methods.

Let me be clear. No legislation proposed in the past, present, or future by a Conservative Government will create powers for police to read emails without a warrant. Our proposed approach of linking an internet address to subscriber information is on par with the phone book linking phone numbers to an address. What this will NOT allow for is access to private communications without a warrant.

That being said, our message is clear: if you use technology to commit crimes like distributing child pornography the police will apprehend you and you will be punished to the fullest extent of the law.

Vic Toews
Minister of Public Safety

Kwavnick, Andrea

From: Christopher Prince [Christopher.Prince@priv.gc.ca]
Sent: November 1, 2011 12:06 PM
To: Kwavnick, Andrea
Subject: RE: Lawful Access
Attachments: 2011-10-31-Letter-to-Ministers-Toews-and-Nicholson-Lawful-Access.pdf

Hi Andrea,

Just as background, I wanted to make sure this letter had made it up to you. It's from the Ont. Office, out yesterday, and goes into more of the details from the provincial perspective I think you'd asked about after the talk at Carleton.

Chris

From: Kwavnick, Andrea [mailto:Andrea.Kwavnick@ps-sp.gc.ca]
Sent: Friday, October 28, 2011 9:53 AM
To: Christopher Prince
Subject: RE: Lawful Access

Hi Chris,

It would be Mike, Michèle, myself and our legal counsel and we envision an informal discussion on certain privacy-related aspects of the former legislation.

Yes we can come to your offices. How about Friday, November 4 from 1:30 - 3:00?

Thanks
Andrea

From: Christopher Prince [mailto:Christopher.Prince@priv.gc.ca]
Sent: October 27, 2011 3:01 PM
To: Kwavnick, Andrea
Subject: RE: Lawful Access

Absolutely, Andrea.

I think Mr. MacDonald and some folks from Justice have been here before on this but we'd gladly sit down next week.

Questions: a) this would be working-level presumably – DG/Dir/you? b) can you come here? c) what days / times next week?

Chris

From: Kwavnick, Andrea [mailto:Andrea.Kwavnick@ps-sp.gc.ca]
Sent: Thursday, October 27, 2011 1:59 PM
To: Christopher Prince
Subject: Lawful Access

000282

25/11/2011

Hi Chris,

Would you be available to further discuss some of the issues we spoke about last week? My Director General, Michael MacDonald, and my Director, Michèle Kingsley, would like to meet with you and members of your team to informally discuss former Bill C-52. In particular, we would like to review some of the issues raised by the Commissioner over the past few years, and most recently in the letter she released today, as well as our thinking on various aspects of the former legislation.

I am hoping we could set something up for late next week.

Please let me know if that works.

Thank you.

Andrea

Andrea Kwavnick

Senior Policy Advisor/Conseiller principal en politiques
National Security Technologies/Technologies de Sécurité Nationale
National Security Operations/Opérations de la Sécurité Nationale
Public Safety Canada/Sécurité Publique Canada
tel: 613.949.6169
Andrea.Kwavnick@ps-sp.gc.ca

Page 284
is a duplicate of
est un duplicata de la
page 375

**Pages 285 to / à 305
are duplicates of
sont des duplicatas des
pages 377 to / à 397**

Scott, Marcie

From: Kwavnick, Andrea
Sent: November 1, 2011 12:15 PM
To: Kingsley, Michèle; Hawrylak, Maciek; Scott, Marcie; Durand, Mathieu; Kousha, Hasti
Subject: FW: Lawful Access
Attachments: 2011-10-31-Letter-to-Ministers-Toews-and-Nicholson-Lawful-Access.pdf
FYI -

Chris Prince from the OPC (who will be attending Friday's meeting) has forwarded a 22-pg letter that Ann Cavoukian (Ontario Privacy Commissioner) sent yesterday to Ministers Toews and Nicholson.

Thanks
Andrea

From: Christopher Prince [mailto:Christopher.Prince@priv.gc.ca]
Sent: November 1, 2011 12:06 PM
To: Kwavnick, Andrea
Subject: RE: Lawful Access

Hi Andrea,

Just as background, I wanted to make sure this letter had made it up to you. It's from the Ont. Office, out yesterday, and goes into more of the details from the provincial perspective I think you'd asked about after the talk at Carleton.

Chris

Page 307
is a duplicate of
est un duplicata de la
page 375

**Pages 308 to / à 328
are duplicates of
sont des duplicatas des
pages 377 to / à 397**

Scott, Marcie

From: Hawrylak, Maciek
Sent: November 1, 2011 2:06 PM
To: Scott, Marcie; Durand, Mathieu; Kwavnick, Andrea; Kousha, Hasti
Subject:
Attachments:
Colleagues,

Thanks,
Maciek

DRAFT – FOR INTERNAL USE ONLY

1 Nov 2011 v1

Review of FPT Privacy Commissioners' conclusions regarding LA Legislation
From Sep 2009 to Nov 2011

Privacy Concern	Solution Proposed by OPC	Our view and solution	Notes
No compelling evidence that new powers are needed	Provide systematic case outlining necessity, legal proportionality, effectiveness, and confirmation of least privacy-invasive solution Lessons of similar initiatives in other countries are considered		Sep 2009 Resolution, Oct 2009 SECU Letter, Mar 2011 Letter, Oct 2011 Letter
New powers should be the least invasive alternative in terms of privacy	Explore alternative to limit powers to emergency situations Proposed powers must be restricted in their application to the investigation of crimes or threats where such an invasion of privacy is justified		Sep 2009 Resolution, Oct 2009 SECU Letter
Ensure appropriate legal thresholds remain in place for court authorization <ul style="list-style-type: none"> Legislation could be used to target even minor infractions and non-criminal matters 	For all activities, do not diminish any thresholds for access to personal information under the proposed bills. For BSI, explore whether judicially-authorized production orders could be obtained, as is done currently in the case of financial institutions under s.487.013 of the <i>Criminal Code</i> . None suggested.		Sep 2009 Resolution, Oct 2009 SECU Letter, Oct 2011 Letter, Mar 2011 Letter

DRAFT – FOR INTERNAL USE ONLY

1 Nov 2011 v1

<ul style="list-style-type: none"> Legal scrutiny will be diminished if the proposals are enacted, and these are ultimately administrative problems that cause delays 	<p>Review the process for court authorization in Canada</p>	
<p>The oversight, reporting and accountability mechanisms must be carefully calibrated to ensure they mirror the breadth and scope of new powers</p>	<p>Generally ensure that the scheme is balanced, and provide for regular public reporting on the use of powers</p>	<p>Sep 2009 Resolution, Oct 2009 SECU Letter, Mar 2011 Letter</p>
<ul style="list-style-type: none"> Audit regime is too arbitrary and subjective 	<ul style="list-style-type: none"> Copies of reports must be given to the Minister and Privacy official, on an annual basis, and with no discretion Agencies should be expressly required to report any collection, use, or retention practices that do not appear to be necessary to the duty or function for which they were originally obtained 	
<ul style="list-style-type: none"> Too many designated officers, not enough resources to offer assurances to Canadians 	<p>Reduce number of designated officers and give federal Privacy Commissioner authority to report on whether privacy officers consider themselves to have adequate resources to conduct audits</p>	

DRAFT -- FOR INTERNAL USE ONLY

1 Nov 2011 v1

<ul style="list-style-type: none"> Not all provincial privacy commissioners have jurisdiction over police forces, or the adequate powers in their acts to investigate police under their jurisdiction 	<p>Create power for Privacy Commissioner to report on where deficiencies exist</p>
<ul style="list-style-type: none"> Review after the fact arrives too late 	<p>None</p>
<p>Improve the consultative and transparency aspects of the bill</p>	<p>Require that draft regulations be reviewed publicly before the legislation comes into force, and include a five-year Parliamentary review</p>
<ul style="list-style-type: none"> Very few privacy organizations have been consulted in this process 	<p>Insist that the relevant federal official re-engage with provincial office of the Attorney-General or territorial equivalents</p>

Sep 2009
Resolution, Oct
2009 SECU
Letter

DRAFT – FOR INTERNAL USE ONLY

1 Nov 20: 1 v1

Drafted: NSOD/Hawrylak
Date: 1 November 2011

Hawrylak, Maciek

From: Hawrylak, Maciek
Sent: November 1, 2011 2:06 PM
To: Scott, Marcie; Durand, Mathieu; Kwavnick, Andrea; Kousha, Hasti
Subject: For Comment: Table summarizing Priv Com concerns re: LA legislation
Colleagues,

Further to yesterday's discussion regarding the Privacy Commissioner's concerns related to LA legislation, please find attached a first draft of the table summarizing their concerns and our responses to those concerns. As I have to get this to Michèle by Wednesday COB, can you please provide any comments by **noon tomorrow**?

For those with access, the document is also found at J:\@09-10 ITTP\LAWFUL ACCESS\STAKEHOLDERS\PRIVACY.

Thanks,
Maciek

DRAFT – FOR INTERNAL USE ONLY

Review of FPT Privacy Commissioners' conclusions regarding LA Legislation
From Sep 2009 to Nov 2011

Privacy Concern	Public Safety Position
Whether all the subscriber identifiers are actually necessary	We should clarify that s. 16 was intended to be an exchange of information – authorities give the TSPs certain identifiers, and in response the TSPs provide certain identifiers. The way the section is currently written makes it appear as though TSPs will be required to provide authorities with all 11 identifiers when in reality this would not be the case.
No compelling evidence that new powers are needed	In most cases, TSPs do provide BSI when it is requested without a warrant. However, those instances when it is not provided can lead to dead end investigations. Furthermore, the fact that in most cases TSPs do provide the information highlights the need to put in place a system of checks and balances that is absent today.
Ensure appropriate legal thresholds remain in place for court authorization	<p>With respect to BSI, there is no legal threshold required in order to obtain the information. PIPEDA currently allows companies to release the information to authorities without a warrant; authorities only need to demonstrate “lawful authority”. There is confusion as to what “lawful authority” means, and so the Government is seeking to clarify - in legislation - that “lawful authority” does not in fact mean a warrant.</p> <p>With respect to the interception of communications, former Bill C-52 did not propose any changes to the authorization processes that currently exist in the <i>Criminal Code</i> or the <i>CSIS Act</i>.</p>
Legislation could be used to target even minor infractions and non-criminal matters	BSI is often used by the police to fulfill non-criminal, policing duties such as returning stolen property or identifying next of kin after a traffic accident. Furthermore, BSI is often necessary in order to prevent a crime, not only to investigate a crime that has already been committed.
Explore whether production orders (s. 487.013 of the <i>Criminal Code</i>) could be obtained in order to access BSI.	BSI is generally ‘visible’ information that does not reveal anything of substance related to the individual. For instance, name, address, and telephone number are all searchable online. A person’s IP address is easy to determine using easily accessible tools, it can appear in some chat rooms and it also tends to be dynamic, in the sense that the IP address is often reassigned to other users when the original user ends his or her session. An email address is equally open, and often handed out by the user. By contrast, s.487.013 compels the release of ‘invisible’ information which reveals personal details regarding an individual. Aside from name and address, s.487.013 could compel the release of a birth date, a bank account number, and

DRAFT – FOR INTERNAL USE ONLY

	the bank account status. This is information normally guarded, rarely handed out, and with potential for substantial financial loss if compromised.
The audit regime is too discretionary and subjective	We could ask what they suggest we do in order to make the regime less discretionary and less subjective.
Too many designated officers, not enough resources to offer assurances to Canadians	The number of BSI requests is dictated by need, not by the number of designated officials. Having fewer designated officials would not lead to fewer requests. In terms of resources, the OPC does not receive additional funding every time a government department or agency implements a program that will be subject to OPC review. It is up to every department to determine how best to allocate their resources.
Not all provincial privacy commissioners have jurisdiction over police forces, or the adequate powers in their acts to investigate police under their jurisdiction	In her annual report to Parliament, the OPC must identify the provincial public officers who will receive the audit reports of the provincial/municipal police forces. She must also report on the powers of these public officers to conduct audits of the police forces with respect to BSI. This function serves to identify any legal or resource issues that could impede the ability of provincial authorities to adequately perform the audits. Because of fed/prov jurisdictional powers, this was as far as the Government could go.
Review after the fact arrives too late	Former Bill C-52 would have put in place an internal oversight mechanism in that only designated officials could have requested BSI, and the requests could only have been made in order to fulfill a function or duty of that particular agency. None of these mechanisms exist today.
Improve the consultative and transparency aspects of the bill	A five-year review is included, and the draft regulations will be reviewed publicly.
Very few privacy organizations have been consulted in this process	Privacy organizations were invited to participate in all of the large-scale consultations, held in 2002, 2005, and 2007. Furthermore, PS has engaged in discussions with the OPC on a number of occasions in the past few years.

DRAFT – FOR INTERNAL USE ONLY

1 Nov 2011 v1

Review of FPT Privacy Commissioners' conclusions regarding LA Legislation
From Sep 2009 to Nov 2011

Privacy Concern	Solution Proposed by OPC	Our view and solution	Notes
<p>No compelling evidence that new powers are needed</p>	<p>Provide systematic case outlining necessity, legal proportionality, effectiveness, and confirmation of least privacy-invasive solution</p>		<p>Sep 2009 Resolution, Oct 2009 SECU Letter, Mar 2011 Letter, Oct 2011 Letter</p>
	<p>Lessons of similar initiatives in other countries are considered</p>		
<p>New powers should be the least invasive alternative in terms of privacy</p>	<p>Explore alternative to limit powers to emergency situations</p>		<p>Sep 2009 Resolution, Oct 2009 SECU Letter</p>
	<p>Proposed powers must be restricted in their application to the investigation of crimes or threats where such an invasion of privacy is justified</p>		
<p>Ensure appropriate legal thresholds remain in place for court authorization</p> <ul style="list-style-type: none"> • Legislation could be used to target even minor infractions and non-criminal matters 	<p>For all activities, do not diminish any thresholds for access to personal information under the proposed bills. For BSI, explore whether judicially-authorized production orders could be obtained, as is done currently in the case of financial institutions under s.487.013 of the <i>Criminal Code</i>. None suggested.</p>		<p>Sep 2009 Resolution, Oct 2009 SECU Letter, Oct 2011 Letter, Mar 2011 Letter</p>

DRAFT – FOR INTERNAL USE ONLY

1 Nov 2011 v1

<ul style="list-style-type: none"> Legal scrutiny will be diminished if the proposals are enacted, and these are ultimately administrative problems that cause delays 	<p>Review the process for court authorization in Canada</p>
<p>The oversight, reporting and accountability mechanisms must be carefully calibrated to ensure they mirror the breadth and scope of new powers</p>	<p>Generally ensure that the scheme is balanced, and provide for regular public reporting on the use of powers</p>
<ul style="list-style-type: none"> Audit regime is too arbitrary and subjective 	<ul style="list-style-type: none"> Copies of reports must be given to the Minister and Privacy official, on an annual basis, and with no discretion Agencies should be expressly required to report any collection, use, or retention practices that do not appear to be necessary to the duty or function for which they were originally obtained
<ul style="list-style-type: none"> Too many designated officers, not enough resources to offer assurances to Canadians 	<p>Reduce number of designated officers and give federal Privacy Commissioner authority to report on whether privacy officers consider themselves to have adequate resources to conduct audits</p>

Sep 2009 Resolution, Oct 2009 SECU Letter, Mar 2011 Letter

DRAFT – FOR INTERNAL USE ONLY

1 Nov 2011 v1

<ul style="list-style-type: none">• Not all provincial privacy commissioners have jurisdiction over police forces, or the adequate powers in their acts to investigate police under their jurisdiction	Create power for Privacy Commissioner to report on where deficiencies exist
<ul style="list-style-type: none">• Review after the fact arrives too late	None
Improve the consultative and transparency aspects of the bill	Require that draft regulations be reviewed publicly before the legislation comes into force, and include a five-year Parliamentary review
<ul style="list-style-type: none">• Very few privacy organizations have been consulted in this process	Insist that the relevant federal official re-engage with provincial office of the Attorney-General or territorial equivalents

Sep 2009 Resolution, Oct 2009 SECU Letter

DRAFT – FOR INTERNAL USE ONLY

1 Nov 2011 v1

Drafted: NSOD/Hawrylak
Date: 1 November 2011

000340

**Pages 341 to / à 342
are duplicates of
sont des duplicatas des
pages 343 to / à 344**

Kingsley, Michèle

From: Kwavnick, Andrea
Sent: November 1, 2011 2:56 PM
To: Kingsley, Michèle; Hawrylak, Maciek; Scott, Marcie; Kousha, Hasti; Durand, Mathieu
Subject: FW: Lawful Access
Privacy Commissioner on CBC...

From: Christopher Prince [mailto:Christopher.Prince@priv.gc.ca]
Sent: November 1, 2011 2:49 PM
To: Kwavnick, Andrea
Subject: RE: Lawful Access

Also this CBC interview with the Commissioner: <http://www.cbc.ca/video/news/audioplayer.html?clipid=2161673582> – on the issue. It's about 14:40 seconds into this section of the show.

From: Kwavnick, Andrea [mailto:Andrea.Kwavnick@ps-sp.gc.ca]
Sent: Tuesday, November 01, 2011 1:31 PM
To: Christopher Prince
Subject: RE: Lawful Access

Hi Chris,

Thanks for sending this along - it hadn't yet made its way to us.

Andrea

From: Christopher Prince [mailto:Christopher.Prince@priv.gc.ca]
Sent: November 1, 2011 12:06 PM
To: Kwavnick, Andrea
Subject: RE: Lawful Access

Hi Andrea,

Just as background, I wanted to make sure this letter had made it up to you. It's from the Ont. Office, out yesterday, and goes into more of the details from the provincial perspective I think you'd asked about after the talk at Carleton.

Chris

From: Kwavnick, Andrea [mailto:Andrea.Kwavnick@ps-sp.gc.ca]
Sent: Friday, October 28, 2011 9:53 AM
To: Christopher Prince
Subject: RE: Lawful Access

Hi Chris,

It would be Mike, Michèle, myself and our legal counsel and we envision an informal discussion on certain privacy-related aspects of the former legislation.

Yes we can come to your offices. How about Friday, November 4 from 1:30 - 3:00?

Thanks
Andrea

From: Christopher Prince [mailto:Christopher.Prince@priv.gc.ca]
Sent: October 27, 2011 3:01 PM
To: Kwavnick, Andrea
Subject: RE: Lawful Access

Absolutely, Andrea.

I think Mr. MacDonald and some folks from Justice have been here before on this but we'd gladly sit down next week.

Questions: a) this would be working-level presumably – DG/Dir/you? b) can you come here? c) what days / times next week?

Chris

From: Kwavnick, Andrea [mailto:Andrea.Kwavnick@ps-sp.gc.ca]
Sent: Thursday, October 27, 2011 1:59 PM
To: Christopher Prince
Subject: Lawful Access

Hi Chris,

Would you be available to further discuss some of the issues we spoke about last week? My Director General, Michael MacDonald, and my Director, Michèle Kingsley, would like to meet with you and members of your team to informally discuss former Bill C-52. In particular, we would like to review some of the issues raised by the Commissioner over the past few years, and most recently in the letter she released today, as well as our thinking on various aspects of the former legislation.

I am hoping we could set something up for late next week.

Please let me know if that works.

Thank you.

Andrea

Andrea Kwavnick

Senior Policy Advisor/Conseiller principal en politiques
National Security Technologies/Technologies de Sécurité Nationale
National Security Operations/Opérations de la Sécurité Nationale
Public Safety Canada/Sécurité Publique Canada
tel: 613.949.6169
Andrea.Kwavnick@ps-sp.gc.ca

Hawrylak, Maciek

From: Paulson, Erika
Sent: November 2, 2011 12:19 PM
To: Kwavnick, Andrea
Cc: 'Audcent, Karen'; 'Shogilev, Matthew'; Patriquin, Kimberly; Burton, Meredith; Kingsley, Michèle; Hawrylak, Maciek
Subject: RE: OPC on CBC

Hi Andrea,
As promised, please find below the transcript of Stoddart's interview with CBC's As It Happens.
Erika

STATION:
CBC RADIO ONE

PROGRAM:
AS IT HAPPENS

TIME:
18:45

LENGTH:
6:30 MINUTES

DATE:
OCTOBER 28, 2011

SUBJECT:
INTERVIEW WITH JENNIFER STODDART

JEFF DOUGLAS (Host): E-snoops, e-spies. Privacy Commissioner Jennifer Stoddart has written an open letter to Public Safety Vic Toews expressing deep concerns about his proposed lawful access legislation. These measures, which did not pass under the previous minority government, would give police and national security agencies new capabilities to conduct digital surveillance. We reached the Privacy Commissioner in Ottawa.

CAROL OFF (Host): Ms. Stoddart, we just cited from your letter that you have deep concerns about the so-called lawful access legislation. Can you outline them for us, please?

JENNIFER STODDART (Privacy Commissioner): Yes. I have concerns that this legislation is going to give police and, you know, enforcement authorities far greater powers to directly access a lot of Canadians' personal information, their email addresses, any information held by their ISPs, cell phone numbers, unlisted numbers and so on, things that we don't normally share with the police, and at the same time, it is reducing the role of the kind of oversight we traditionally enjoyed in Canadian society, which has been provided through the judicial oversight and the warrant system.

CAROL OFF: That oversight is, of course, that when they want to do a search of our house, our property, police must go and get a search warrant for that.

JENNIFER STODDART: Exactly, and traditionally our correspondence too has a high degree of privacy, and it's this lack of judicial oversight at the initial stages that is of great concern, and as I say, there's going to be a lot of information that is now present because of the dominant electronic way in which most of us are now communicating, that will be directly accessible by the police.

CAROL OFF: Can you give some scenarios in which you think police will be using this legislation, if they have it?

JENNIFER STODDART: I think they're going to be using it for ongoing law enforcement scenarios. However, one of the things that I've been saying, and privacy commissioners across Canada join me in

000345

24/11/2011

this, is that, you know, we've never really heard a compelling case on which exact type of problems these new enforcement powers would make a significant difference. You know, we hear about dramatic examples, the child abuse cases and children being tortured online and so on, but we have no problem with emergency situations, emergency authority and so on. But one of the things that we find puzzling is that there hasn't been a case with numbers that shows us in how many cases was the lack of greater enforcement powers a significant factor in combating crime.

CAROL OFF: Is it your understanding that it would be used in their investigating a crime, or might it be used to actually monitor, track people, know their whereabouts, their activities, even if they don't know that that person is involved in crime?

JENNIFER STODDART: Well, exactly, Carol, and I think you've put your finger on it. The reason that there is no answer to this question, show us the difference it would make, is because right now they don't have this power to just generally track us, you know, through our email traffic, through our envelope data on the Internet, and so it's going to give the police new general surveillance powers to look at patterns of communication that they can't look at now. And I think that is where it becomes very, very concerning from our privacy point of view, because that means potentially all citizens, not just people who are suspected of something, but all citizens then could have their communications traffic monitored.

CAROL OFF: It's a very Orwellian picture you're painting.

JENNIFER STODDART: Well, it is. It would be much less Orwellian if there was more implication of the judiciary, there were some other alternate form of oversight, like a special commissioner, like the way we have for, you know, CSIS has its own special committee. In this proposed bill, or the one we saw in the last Parliament, there's a remarkable lack of transparency, and there is virtually no oversight.

CAROL OFF: But I guess one of the arguments the government is giving is that the way that information moves around, the way criminals can now access data around the world, move images around, that the police can't be hamstrung by oversight of this nature, that if they have to go through a cumbersome process in order to get their permission, then they'll slow them down in their crime fighting.

JENNIFER STODDART: Well, you know, certainly I'm the first to admit that the nature of communication has changed, but what I don't accept is that because it changes, we cannot adapt the processes that ensure our democratic rights, one of the most important of which is privacy, which, you know, gives us the space in which to express our thoughts, to be autonomous individuals, to, you know, have a free and open society. What I see in these bills, that there's been no serious attempt to look at an appropriate 21st century oversight regime.

CAROL OFF: Now, one often hears Canadians who are prepared, they say they're prepared to give up a lot of privacy if they believe it will help to prevent the spread of things like child pornography, and child pornography's one of the things the Minister says is a major target. Is public opinion on your side?

JENNIFER STODDART: The public opinion polling that we've done, Carol, shows that Canadians are very, very concerned. As I remember, a majority of Canadians are concerned about the possible erosion of their privacy through greater police enforcement power. So I think there is a groundswell of concern across Canada.

CAROL OFF: Do you know if the legislation will have the problems in it that you found in previous drafts of this? I mean, this is... we haven't seen this yet, so how do you know your concerns haven't been answered?

JENNIFER STODDART: Well, that's what I'm hoping, that in fact someone is listening to my concerns, and I am heartened by the fact that this legislation has not been reintroduced so far, and in the format in which it was last spring, and I know that sometime in the near future, more discussions are planned with Minister Toews' department, and I'm hoping that, you know, we could discuss some alternate approaches to part of this legislation.

CAROL OFF: All right, we'll be watching for the legislation. Ms. Stoddart, thank you.

JENNIFER STODDART: Thank you, Carol. Bye-bye.

CAROL OFF: Bye-bye.

JEFF DOUGLAS: From Ottawa, that was Canada's Privacy Commissioner Jennifer Stoddart.

This transcription has been prepared by an outside supplier exclusively for departmental employees. Copyright laws prevent redistribution outside of Public Safety. Cette transcription a été préparée par un fournisseur externe exclusivement pour les employés du Ministère. Les lois sur le droit d'auteur en empêchent la diffusion à l'extérieur de la Sécurité publique.

From: Paulson, Erika
Sent: Tuesday, November 01, 2011 4:18 PM
To: Kwavnick, Andrea
Cc: 'Audcent, Karen'; 'Shogilev, Matthew'; Patriquin, Kimberly; Burton, Meredith
Subject: RE: OPC on CBC

Thanks, Andrea. Comms is waiting on a transcript of this interview and will share once it's in.

FYI – I think this may be the polling the Privacy Commissioner refers to in her interview:
http://www.priv.gc.ca/information/survey/2011/por_2011_01_e.pdf

EXCERPT:

Privacy and New Technologies

Privacy concerns related to Internet, computers, public Wi-Fi, social networking are on the rise:

Most Canadians (82%) did not feel that police and intelligence agencies should be able to request information from telecommunications companies about Canadians and their internet usage without a warrant issued by the courts.

Erika Paulson
Tel: 613-993-4415

From: Kwavnick, Andrea
Sent: Tuesday, November 01, 2011 3:35 PM
To: Paulson, Erika; Burton, Meredith; 'Audcent, Karen'; 'Shogilev, Matthew'
Subject: OPC on CBC

Good Afternoon,

A CBC interview with the Privacy Commissioner: <http://www.cbc.ca/video/news/audioplayer.html?clipid=2161673582> – on Lawful Access - about 14:40 into the show.

Thanks
Andrea

Scott, Marcie

From: Kousha, Hasti
Sent: November 2, 2011 1:29 PM
To: Scott, Marcie
Subject: RE:

Attachments:

Hi Marcie,

Thank you,
Hasti

From: Scott, Marcie
Sent: November 2, 2011 12:58 PM
To: Kousha, Hasti
Subject: RE:

Marcie Scott
613-949-5886

From: Kousha, Hasti
Sent: November 2, 2011 11:58 AM
To: Scott, Marcie
Subject: RE:

Ok,

From: Scott, Marcie
Sent: November 2, 2011 11:57 AM
To: Kousha, Hasti
Subject: RE:

Hi,

Marcie Scott
613-949-5886

From: Scott, Marcie
Sent: November 2, 2011 11:10 AM
To: Kousha, Hasti
Subject:

Hi Hasti,

Thank you,

Marcie Scott

Policy Coordinator | Coordinatrice de politiques
National Security Operations | Opérations de la sécurité nationale
Emergency Management and National Security Branch |
Secteur de la gestion des urgences et de la sécurité nationale
Public Safety Canada | Sécurité publique Canada

Tel: 613-949-5886

**Pages 350 to / à 351
are withheld pursuant to section
sont retenues en vertu de l'article**

**of the Access to Information
de la Loi sur l'accès à l'information**

**Pages 352 to / à 354
are duplicates of
sont des duplicatas des
pages 355 to / à 357**

**Pages 355 to / à 357
are not relevant
sont non pertinentes**

**Pages 358 to / à 360
are not relevant
sont non pertinentes**

Kingsley, Michèle

From: Kingsley, Michèle
Sent: November 3, 2011 4:49 PM
To: Kwavnick, Andrea
Subject: Re: table

Thanks. I think I was able to read it all. Looks good. Thanks for turning it around so quickly.

From: Kwavnick, Andrea
Sent: Thursday, November 03, 2011 04:45 PM
To: Kingsley, Michèle
Subject: table

I made changes to the table. I'm not sure how well you can read it on your bb - but here it is.

Privacy Concern	Public Safety Position
Whether all the subscriber identifiers are actually necessary	We should clarify that s. 16 was intended to be an exchange of information <input type="checkbox"/> authorities give the TSPs certain identifiers, and in response the TSPs provide certain identifiers. The way the section is currently written makes it appear as though TSPs will be required to provide authorities with all 11 identifiers when in reality this would not be the case.
No compelling evidence that new powers are needed	In most cases, TSPs do provide BSI when it is requested without a warrant. However, those instances when it is not provided can lead to dead end investigations. Furthermore, the fact that in most cases TSPs do provide the information highlights the need to put in place a system of checks and balances that is absent today.
Ensure appropriate legal thresholds remain in place for court authorization	With respect to BSI, there is no legal threshold required in order to obtain the information. PIPEDA currently allows companies to release the information to authorities without a warrant; authorities only need to demonstrate <input type="checkbox"/> lawful authority <input type="checkbox"/> . There is confusion as to what <input type="checkbox"/> lawful authority <input type="checkbox"/> means, and so the Government is seeking to clarify - in legislation - that <input type="checkbox"/> lawful authority <input type="checkbox"/> does not in fact mean a warrant. With respect to the interception of communications, former Bill C-52 did not propose any changes to the authorization processes that currently exist in the <i>Criminal Code</i> or the <i>CSIS Act</i> .
Legislation could be used to target even minor infractions and non-criminal matters	BSI is often used by the police to fulfill non-criminal, policing duties such as returning stolen property or identifying next of kin after a traffic accident. Furthermore, BSI is often necessary in order to prevent a crime, not only to investigate a crime that has already been committed.
Explore whether production orders (s. 487.013 of the <i>Criminal</i>	BSI is generally <input type="checkbox"/> visible <input type="checkbox"/> information that does not reveal anything of substance related to the individual. For instance, name, address, and telephone number are all searchable

<p>Code) could be obtained in order to access BSI.</p>	<p>online. A person's IP address is easy to determine using easily accessible tools, it can appear in some chat rooms and it also tends to be dynamic, in the sense that the IP address is often reassigned to other users when the original user ends his or her session. An email address is equally open, and often handed out by the user. By contrast, s.487.013 compels the release of "invisible" information which reveals personal details regarding an individual. Aside from name and address, s.487.013 could compel the release of a birth date, a bank account number, and the bank account status. This is information normally guarded, rarely handed out, and with potential for substantial financial loss if compromised.</p>
<p>The audit regime is too discretionary and subjective</p>	<p>We could ask what they suggest we do in order to make the regime less discretionary and less subjective.</p>
<p>Too many designated officers, not enough resources to offer assurances to Canadians</p>	<p>The number of BSI requests is dictated by need, not by the number of designated officials. Having fewer designated officials would not lead to fewer requests.</p> <p>In terms of resources, the OPC does not receive additional funding every time a government department or agency implements a program that will be subject to OPC review. It is up to every department to determine how best to allocate their resources.</p>
<p>Not all provincial privacy commissioners have jurisdiction over police forces, or the adequate powers in their acts to investigate police under their jurisdiction</p>	<p>In her annual report to Parliament, the OPC must identify the provincial public officers who will receive the audit reports of the provincial/municipal police forces. She must also report on the powers of these public officers to conduct audits of the police forces with respect to BSI. This function serves to identify any legal or resource issues that could impede the ability of provincial authorities to adequately perform the audits. Because of fed/prov jurisdictional powers, this was as far as the Government could go.</p>
<p>Review after the fact arrives too late</p>	<p>Former Bill C-52 would have put in place an internal oversight mechanism in that only designated officials could have requested BSI, and the requests could only have been made in order to fulfill a function or duty of that particular agency. None of these mechanisms exist today.</p>
<p>Improve the consultative and transparency aspects of the bill</p>	<p>A five-year review is included, and the draft regulations will be reviewed publicly.</p>
<p>Very few privacy organizations have been consulted in this process</p>	<p>Privacy organizations were invited to participate in all of the large-scale consultations, held in 2002, 2005, and 2007. Furthermore, PS has engaged in discussions with the OPC on a number of occasions in the past few years.</p>

**Pages 363 to / à 364
are duplicates of
sont des duplicatas des
pages 335 to / à 336**

Oversight and Review

The Office of the Privacy Commissioner of Canada (OPC) has expressed concern that “review [of the collection and use of basic subscriber information or BSI] after the fact is too late”, presumably calling for external (judicial) oversight during the collection and use of this information.

We presume that in the context of the OPC’s comment, **review** refers to an examination of actions after the fact. It is our understanding that oversight refers to actions taken to account for actions either in advance or at the time that said actions occur.

However, we propose that oversight and review mechanisms are not always mutually exclusive, in that review may be part of an oversight regime.

Former Bill C-52 would have employed internal review, internal oversight, and external review mechanisms. The definitions for the purposes of this discussion are as follows:

- **Internal oversight:** Actions taken by an organization to account for actions either in advance or at the time that they occur, such as the implementation and adherence to policies related to the collection and use of information.
- **Internal review:** A review of actions that occurred in the past conducted by the organization that took the action, to identify any recurring issues and ensure that any necessary corrective action is taken.
- **External review:** A review of actions that occurred in the past conducted by a body that has been given the authority to independently review or report on past actions of another organization, to identify any recurring issues and recommend corrective action.

External oversight refers to oversight activities conducted by a body to account for actions either in advance or at the time that they occur.

OPC

The mandate of the Office of the Privacy Commissioner of Canada (OPC) is to oversee compliance with the *Privacy Act*, for federal government departments, and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), for the private sector. The OPC is an external body that works independently from any other part of the government to investigate complaints from individuals with respect to the federal public sector and the private sector.

Among other responsibilities, the OPC investigates complaints and issues reports with recommendations to federal government institutions and private sector organizations to remedy situations, as appropriate; and, assesses compliance with obligations contained in the *Privacy Act* and PIPEDA through the conduct of independent audit and review activities, and publicly reports on findings.

The *Privacy Act* does not use the terminology “oversight” in the context of the Privacy Commissioner’s duties, but does refer to “review” often.

Presumably, federal bodies who are required to be compliant with the *Privacy Act* would have continued to be so if former Bill C-52 had passed. Thus, the OPC would have continued to have jurisdiction to receive and investigate complaints related to privacy as well as to report on any issues they felt were relevant.

CSIS and RCMP

In the national security context and law enforcement context, external review mechanisms exist to examine past actions of CSIS and the RCMP.

SIRC

The Security Intelligence Review Committee (SIRC) handles complaints against CSIS and also undertakes regular reviews of CSIS activities, as per authority given in section 38 of the *CSIS Act*. SIRC does not provide internal oversight of CSIS actions. Their reviews serve to advise and provide non-binding recommendations to CSIS. Under section 20(5) of former Bill C-52, SIRC would have been responsible for reviewing (after the fact) the collection and use of BSI.

CPC

The Commission for Public Complaints Against the RCMP (CPC) is an independent agency created by Parliament that receives and reviews complaints against the RCMP, investigates and/or holds hearings related to complaints as necessary, and reports on findings and makes recommendations. A complaint can be initiated by a member of the public or by the Commissioner of the RCMP. The CPC does not provide internal oversight of the RCMP. The Commission’s reports aim to correct past issues in order to promote excellence in policing through accountability.

Internal and External Review and Oversight in Former Bill C-52

Former Bill C-52 would have provided a number of oversight and review mechanisms for basic subscriber information, namely:

- Internal oversight: The former Bill would have required police, CSIS and the Competition Bureau to identify a limited number of designated officials who could make requests for BSI. The only exception to this would be if a police officer required information in an emergency situation. In all cases, each time that a request is made, a record would have needed to be created and retained, and the information must be used in a manner consistent to its collection.
- Internal review: The former Bill would have required police, CSIS and the Competition Bureau to undertake regular internal audits of the practices of his or her agency to ensure compliance with the provisions related to access to BSI, designated officials’ access and exceptional circumstance requests, and the

regulations made for the purposes of those sections, and of the internal management and information systems and controls concerning requests made.

- External review: The former Bill would have required reviews to be undertaken by privacy commissioners (for police and Competition Bureau) and SIRC (for CSIS). Any issues related to the collection and use of BSI would be documented, and recommendations made could be used to inform improvements in the processes related to the handling of said information.
- That being said, we propose that the findings and recommendations related to these reviews, as well as those in the CPC's reports, although not binding, contribute to an overall oversight regime. Any issues related to the collection and use of BSI would be documented, and recommendations made could be used to inform improvements in the processes related to the handling of said information. The frequency in which these reviews or reports may occur could lend to how reliable they are as part of an oversight regime.

Former Bill C-52 would not have provided the external oversight that we believe the OPC is referring to, which is judicial oversight. Officials are preparing an explanation of why it is not feasible to use warrants to access basic subscriber information.

Page 368

**is withheld pursuant to section
est retenue en vertu de l'article**

**of the Access to Information
de la Loi sur l'accès à l'information**

Access to Basic Subscriber Information

The OPC has criticized the government's intention to provide for warrantless access to Basic Subscriber Information (BSI) and has suggested various alternatives. These alternatives, as well as an explanation as to why they are not suitable, are provided below.

Requiring a Warrant to Access BSI

The OPC has consistently called on the Government to require authorities to obtain judicial authority (i.e. a warrant) in order to access basic subscriber information (BSI).

This would not be feasible for the following reasons:

- Thousands of requests are processed across Canada every year. To move this into the courts would literally collapse an already over-burdened judicial system as the resource and logistics requirements would be impractical.
- BSI is often the most basic piece of information needed to obtain a warrant. Lack of timely access to this information can, and often does, block investigations.
- Warrants are generally granted for criminal investigations. Requiring a warrant would be problematic when police undertake non-criminal, general policing duties – such as contacting next-of-kin after a traffic accident or returning stolen property.
- The type of information obtained from BSI is significantly less intrusive compared to that which is obtained with a warrant.

Requiring a Warrant to Access BSI in Non-Emergencies

The OCP has suggested that a warrant be required in order to access BSI in non-emergencies.

This would not be feasible for the following reasons:

- It could limit the ability of police to access BSI in non-emergencies
- It could undermine the ability of CSIS to access BSI
- It could limit the ability of police to fulfill non-criminal, general policing duties such as returning stolen property, identifying next of kin after a traffic accident or responding to individuals threatening suicide online

Personal Information Protection and Electronic Documents Act (PIPEDA)

Some privacy advocates believe that there is currently a warrant requirement to obtain BSI. While the OPC seems to understand that is not the case, it may be useful to highlight that PIPEDA allows TSPs to provide BSI to authorities without a warrant.

There are two problems with PIPEDA with respect to BSI:

- PIPEDA requires that authorities demonstrate "lawful authority" to collect BSI, which is interpreted by some TSPs to mean a warrant
- PIPEDA allows TSPs to share BSI with authorities, but does not compel them to do so

A Bill seeking to amend PIPEDA is currently before Parliament (Bill C-12). While the legislation would clarify that the concept of "lawful authority" does not require authorities to have a warrant, the voluntary aspect would remain.

DRAFT - UNCLASSIFIED

Access to Basic Subscriber Information

The OPC has criticized the government's intention to provide for warrantless access to Basic Subscriber Information (BSI) and has suggested various alternatives. These alternatives, as well as an explanation as to why they are not suitable, are provided below.

Requiring a Warrant to Access BSI

The OPC has consistently called on the Government to require authorities to obtain judicial authority (i.e. a warrant) in order to access basic subscriber information (BSI). This would not be feasible for the following reasons:

- Thousands of requests are processed across Canada every year. To move this into the courts would literally collapse an already over-burdened judicial system as the resource and logistics requirements would be impractical.
- BSI is often the most basic piece of information needed to obtain a warrant. Lack of timely access to this information can, and often does, block investigations.
- Warrants are generally granted for criminal investigations. Requiring a warrant would be problematic when police undertake non-criminal, general policing duties – such as contacting next-of-kin after a traffic accident or returning stolen property.
- The type of information obtained from BSI is significantly less intrusive compared to that which is obtained with a warrant.

Requiring a Warrant to Access BSI in Non-Emergencies

The OPC has also suggested that the Government provide for warrantless access to BSI only in emergencies, and require authorities to obtain a warrant in non-emergency situations.

If the Government were to adopt this system, there is concern that TSPs could interpret their obligations to provide the information as limited to emergencies and would no longer provide authorities with BSI requested under PIPEDA in non-emergency situations (without a warrant). This could negatively impact the agencies for the following reasons:

- It could limit the ability of police to access BSI in non-emergencies
- It could undermine the ability of CSIS to access BSI
- It could limit the ability of police to fulfill non-criminal, general policing duties such as returning stolen property or identifying next of kin after a traffic accident

A conference call between FPT Deputy Ministers responsible for Justice and Public Safety is scheduled for May 19th. An issue that may be raised during the discussion is the criticisms brought forward by the Federal and Provincial Privacy Commissioners concerning former Bill C-52, the *Investigating and Preventing Criminal Electronic Communications Act* and former Bill C-51, the *Investigative Powers for the 21st Century Act*. In particular, Jennifer Stoddart and her provincial counterparts sent Deputy Minister Baker a letter in March 2011 expressing concerns with the former legislation. This letter is now posted on the Privacy Commissioner's website.

If this issue is raised, you may wish to use the following speaking points:

- Government officials have consulted with Privacy Commissioners regarding lawful access legislation and have always conveyed our intention to balance the privacy rights of Canadians with the investigative and policing requirements of national security and law enforcement agencies. The comments and advice received from the Privacy Commissioners over the years have informed lawful access legislation and will continue to contribute to this important initiative.
- On December 15, 2010, officials from the Department of Justice and Public Safety Canada, including the Deputy Minister, met with Jennifer Stoddart to discuss former Bill C-52. Following this meeting, Privacy Commissioners sent a letter reiterating their concerns, which was recently posted on the Internet. The Deputy Minister's response letter indicated that the need for lawful access legislation has been clearly demonstrated by national security and law enforcement agencies across the country, that we fully appreciate the need to strike the right balance between the privacy of Canadians and investigative and policing requirements and that Privacy Commissioners' suggestions will inform Public Safety Canada's advice to the Government on a potential new iteration of lawful access legislation.
- Former Bill C-52 died on the Order Paper with the dissolution of Parliament. The Bill could be included in an omnibus crime bill that the Government committed to pass within the first 100 sitting days of Parliament.
- If lawful access legislation is reintroduced, we might engage Privacy Commissioners again to clarify the need for the Bill and highlight the privacy safeguards it contains.

Veilleux, Martine

From: Donato, Renée on behalf of Baker, William V.
Sent: Tuesday, November 01, 2011 4:55 PM
To: MacKinnon, Paul
Cc: Clairmont, Lynda; Veilleux, Martine; Perry, Gates; Coburn, Stacey; Piasko, Ruba; Dupuis, Chantal; Dussault, Josée; Robert, Philippe; Lozier, Marie-France; Donato, Renée; Saunders, Joanne
Subject: FW: 383494: CORRECTED PDF for Privacy Implications of Expanded Surveillance - Letter from Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario
Attachments: 2011 October 31 Letter to Ministers Toews and Nicholson reSurveillance.pdf; 383494: Privacy Implications of Expanded Surveillance - Letter from Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario
Importance: High

Good afternoon,
Please see attached correspondence for your information.
Paper docket to follow shortly.
Thank you

Renée Donato

A / Executive Assistant to the Deputy Minister / Adjointe exécutive du Sous-ministre / I
Public Safety Canada / Sécurité publique Canada
269 Laurier Avenue West / 269, avenue Laurier Ouest
Ottawa ON K1A 0P8
Tel: 613-991-2891 Fax: 613-990-8312

From: Debra Adair [mailto:Debra.Adair@ipc.on.ca]
Sent: October 31, 2011 4:48 PM
To: 'vic.toews@parl.gc.ca'; 'Nichor@parl.gc.ca'
Cc: 'john.gerretsen@ontario.ca'; 'murray.segal@ontario.ca'; 'johanne.rousseau@justice.gc.ca'; Baker, William V.
Subject: 383494: CORRECTED PDF for Privacy Implications of Expanded Surveillance - Letter from Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario
Importance: High

Dear Ministers,

Please find attached a corrected version of the letter sent to you earlier today from Commissioner Cavoukian regarding privacy implications of expanded surveillance. The same letter will also arrive by courier on Tuesday to your office.

My apologies for any inconvenience.

Regards,

Debra Adair
Administrative Assistant to Dr. Ann Cavoukian, Commissioner
Office of the Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Office: 416-326-3936 (direct)

Fax: 416-212-6523 (office fax)

TTY: 416-325-7539



www.privacybydesign.ca

You can also follow Privacy by Design on Twitter [@embedprivacy](https://twitter.com/embedprivacy)



Information and Privacy
Commissioner of Ontario
Commissaire à l'information
et à la protection de la vie privée de l'Ontario

October 31, 2011

VIA ELECTRONIC MAIL AND COURIER

The Honourable Vic Toews
Minister of Public Safety
269 Laurier Avenue West
Ottawa, Canada
K1A 0P8

The Honourable Robert Nicholson
Minister of Justice and Attorney General of Canada
284 Wellington Street
Ottawa, Ontario
K1A 0H8

Dear Ministers:

Introduction

As the Information and Privacy Commissioner of Ontario, I felt compelled to write to you today regarding the federal government's insistence on enacting a highly intrusive surveillance regime. I do so in full support of Canada's Privacy Commissioner Stoddart and the open letter she sent to Minister Toews on October 26th.

At the outset, please note that my mandate includes commenting on developments that affect the personal privacy of Ontarians, and overseeing law enforcement compliance with privacy legislation in Ontario. The proposed surveillance regime will have a substantial impact on the privacy rights of Ontarians, law enforcement functions, and the role of my office.

Media reports referring to Minister Toews' rejection of Commissioner Stoddart's concerns and quoting his defence of the regime suggest that the government will re-introduce Bills C-50, C-51, and C-52 ("the Bills") in essentially the same form in which they appeared in the last Parliament. In my view, that would be highly regrettable for the people of Ontario and Canada. I am writing this open letter to outline my specific concerns and concrete recommendations.

I have first summarized the privacy concerns identified by my office into five categories, followed by an in-depth discussion of each.

.../2



2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel: 416-326-3333
1-800-387-0073
Fax/Téloc: 416-325-9188
TTY: 416-325-7539
www.ipc.on.ca

000375

Summary of Privacy Concerns:

Reconsidering the Privacy Implications of Expanded Surveillance and Access

Before providing a detailed analysis of the privacy issues, my concerns may be summarized as follows:

- 1) The proposed powers must not come at the expense of the necessary privacy safeguards guaranteed under the *Canadian Charter of Rights and Freedoms*; in order to maintain the integrity of this constitutional framework, the government must acknowledge the sensitivity of traffic data, stored data, and tracking data.
- 2) Intrusive proposals require essential matching legislative safeguards; the courts, affected individuals, future Parliaments, and the public must be well informed about the scope, effectiveness, and deleterious effects of intrusive powers. If Parliament enacts expansive new surveillance powers, we urge the federal government to publicly commit to enacting the necessary oversight legislation in tandem.
- 3) Even with matching oversight, the proposed surveillance and access powers will require more stringent conditions precedent to determine the situations when surveillance or access may be appropriate and necessary.
- 4) The government must not impose a mandatory surveillance capacity regime on the public and its telecommunication service providers (TSPs) without adequate safeguards to protect the future of freedom and privacy; a comprehensive and public cost-benefit analysis should precede rather than follow the making of so many significant public policy decisions. Public Parliamentary hearings should be scheduled to ensure that civil society, as well as industry, have a full opportunity to provide substantial input on all of the Bills including Bill C-52 (the *Electronic Communications Act*). In addition, the *Electronic Communications Act* should be amended to require that all interception-related capacity requirements be approved by Parliament before they can be imposed.
- 5) The proposal for warrantless access to subscriber information is untenable and should be withdrawn; it remains our view that the *Electronic Communications Act* should be amended to require that the provisions setting out TSP obligations concerning "subscriber information" be deleted and replaced with a court supervised regime.

.../3

1) New Powers Must Not Come at the Expense of the Constitutional Framework

In a steady stream of communiqués dating back almost a decade and spanning 2002, 2005, 2007, 2009, and 2011, our office has cautioned against taking a legislative approach to new surveillance powers that undermines the judicially supervised rules and procedures which secure our shared rights to privacy, freedom and security of the person. Two of these were in joint communiqués led by the Privacy Commissioner of Canada, and signed by all the provincial and territorial privacy commissioners and ombudsmen (“privacy commissioners”).¹

Together, they accurately reflect the general nature of many of our current concerns and recommendations. (We also urge you to carefully consider the federal Privacy Commissioner’s November 2010 publication *A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century*.)

The concerns voiced by Canada’s privacy commissioners have been echoed by legal and academic experts specializing in technology, privacy and the law and, most importantly, by thousands of concerned Canadians who wish to have both effective law enforcement *and* strong privacy protections.

In this context, there can be little doubt that the most recent iteration of the government’s approach to expansive surveillance legislation has significant implications for personal privacy, state powers, and the longstanding constitutional compromise between the two, as well as for the oversight functions of courts and privacy commissioners, and the future of innovation, costs and competitiveness in the communications and technology fields.

The fact that the government appears to be committed to limiting real-time surveillance of private communications including in-transit e-mail under the “wiretapping” rules set out in Part VI of the *Criminal Code* is welcome news. We also welcome the absence of any public call for the creation of data retention rules with respect to subscribers and their day-to-day use of the new technologies. No such retention rules should be countenanced.

At the same time, we believe that critical elements of the proposed legislative regime suggest that the government misconceives how Canadians interact with new communications technologies and significantly underestimates the sensitivity of the personal information involved. The concomitant risks to privacy and other fundamental rights are significant.

¹ Copies of these five communiqués are available at:
December 20, 2002 - <http://www.ipc.on.ca/english/Resources/Reports-and-Submissions/Reports-and-Submissions-Summary/?id=114>; April 21, 2005 - <http://www.ipc.on.ca/english/Resources/Reports-and-Submissions/Reports-and-Submissions-Summary/?id=105>; October 10, 2007 - <http://www.ipc.on.ca/english/Resources/Reports-and-Submissions/Reports-and-Submissions-Summary/?id=662>; September 9-10, 2009 - http://www.priv.gc.ca/media/nr-c/2009/res_090910_e.cfm; and March 9, 2011 - http://www.priv.gc.ca/media/nr-c/2011/let_110309_e.cfm.

- 4 -

Why? Because new surveillance powers leverage new and still evolving technologies. As a result, they significantly *increase* rather than merely maintain the state's surveillance capacity. Accordingly, attempts to frame the public debate in terms of maintaining capacity are misleading:

The ways in which we communicate with each other have undergone such enormous changes that it is entirely fanciful to say that there are simple equivalents in the Internet and broader digital domain to the communications surveillance techniques used for conventional voice-based telephones. There are many new types of communication available between individuals, but nearly all of these are in forms that are very easily computer-readable and therefore capable of complex analysis by computers. The range of tools available to law enforcement to track and link activity and database content is now vast and growing all the time. The debate is thus not about maintenance of capability but trying to determine a proper balance in new circumstances.²

In this context, the legal distinction traditionally drawn between the content of a private communication such as is exchanged during a telephone call or via e-mail and the associated *traffic* data is being overtaken by social, economic and technological developments. What we refer to as traffic data has evolved and it will continue to do so. Certainly, it is no longer confined to a list of phone numbers obtained by a dial recorder or rows of text on a telephone bill.

It extends digitally to link and trace the ongoing interactions of networks of users through unique identifying device numbers *vis-à-vis* their location in time, their location on and along the ground, their activity and interactivity within the Internet, and their relatedness within and across communities. The resulting digital trails are routinely retained by service providers and various third parties for weeks, months or even years. These trails paint a detailed and evolving picture that reflects on who we are.

Furthermore, there are strong indications that law enforcement's appetite for the surveillance of live telephone communications is being dwarfed by their interest in accessing the private content in the mass of digital trails created every time an individual sends a message, surfs the Internet, e-banks or simply carries a 3G enabled device.³ Computer facilitated analysis of this data can readily reveal the interwoven layers of core biographical information that animate communications data, particularly where the scrutiny extends for a significant period of time. As recognized by the United States Court of Appeals for the District of Columbia in a Fourth Amendment GPS vehicle tracking case being heard by the U.S. Supreme Court on November 8, 2011:

² London School of Economics, *Briefing on the Interception Modernisation Programme*, June 2009, p. 6.

³ See "The Law Enforcement Surveillance Reporting Gap" by Christopher Soghoian, Indiana University Bloomington - Center for Applied Cybersecurity Research, April 10, 2011.

.../5

Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynaecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups — and not just one such fact about a person, but all such facts.⁴

Properly supervised, surveillance powers can be invaluable to law enforcement. However, it is equally true that where individuals are subject to unwarranted suspicions, evidence is poorly handled, or erroneous conclusions are hastily drawn, the consequences for innocent individuals can be devastating. Recent national security-related investigations make this all too clear (*e.g.*, Maher Arar).

While we continue to support the vital law enforcement interest in pursuing electronic evidence and intelligence about serious wrongdoing, we also urge the government to ensure that any search, seizure, or surveillance of personal communications be subject to the most rigorous oversight. The constitutional values at stake demand such safeguards.

On the basis of all the above, we reject the Bills' implicit claim that the so-called non-content data elements associated with new communication devices and services are of significantly lesser constitutional significance. Safeguards comparable to those necessary to properly regulate the wiretapping of a rotary phone are required with respect to 21st century communications, including, but not limited to, rigorous prior judicial scrutiny.

2) Intrusive Proposals Require Essential Matching Legislative Safeguards

Read together, the legislative proposals substantially diminish the privacy rights of Canadians. They do so by enhancing the capacity of the state to conduct surveillance, as well as access private information, while *reducing the frequency and vigour of judicial scrutiny*, thus making it easier for the state to subject more individuals to surveillance and scrutiny.

Are the current processes that provide for oversight of surveillance-related powers sufficient to keep pace with the proposed expansion of state power? With the anticipated re-introduction of the Bills, Canadians are being asked to rely on oversight regimes designed decades ago to provide sufficient safeguards for the protection of our fundamental rights and freedoms today.

⁴ *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), cert. granted, *United States v. Jones*, 2011 WL 1456728 (June 27, 2011), U.S.S.C. Docket No. 10-1259.

The supervision provided by prior judicial authorization, the criminal trial process, and complaint-driven oversight under police and privacy-related statutes, while critical, are fundamentally insufficient. Let me explain.

The proposed surveillance and access regime will frequently involve complex, highly technical, and sensitive information. Moreover, where prior judicial authorization is required, the relevant surveillance and access applications are necessarily held *in camera* and *ex parte*. Where the resultant surveillance and access activities produce legal charges that lead to a criminal trial, the trials invariably have a narrow focus on the accused. National security-related investigations, which often have a much broader focus, invariably proceed in secrecy, and are rarely subject to public scrutiny. In both contexts, innocent individuals subject to surreptitious invasions of their privacy may never be in a position to learn about, let alone file for or find any redress. In addition, existing complaint regimes are limited as to their reach, powers and remedies. Any in depth public scrutiny of such matters will be the *rare* exception to a general rule of confidentiality and secrecy.

Furthermore, under the Bills, local, provincial, and federal law enforcement agencies will be equally empowered to use these intrusive powers in pursuit of both domestic and international investigations. Without a focused harmonizing and coordinating authority, inconsistent policies and practices are likely to develop among the various jurisdictions. Inevitably, privacy rights and civil liberties will suffer from fragmented and inconsistent protections.

Canadians have a *constitutional* right to be secure from unreasonable search and seizure. The expansive surveillance proposals bring this right into question. And, since the state's authority to intrude on privacy does not come with concomitant responsibilities with respect to accountability, notification and transparency, the net negative effect on human rights is likely to be compounded over time.

To its credit, the government has responded to recent court rulings⁵ by including a provision in Bill C-50 that will require that: (i) a person who has been the target of a warrantless exceptional circumstances interception must be notified of the interception within a specified period; and (ii) the relevant Minister must report publicly on police resort to such warrantless wiretaps.

At the same time, we note that these notice and reporting mechanisms are confined to providing a modest degree of notice, transparency and accountability (restricted as they are to only notifying the *target* of the surveillance, and confined as they are to limited numeric reporting) with respect to a single surveillance power – the power to intercept a private communication. In addition, the reporting practices of provincial and federal Attorneys General with respect to the use of these Part VI wiretap powers have varied considerably (as seen in jurisdictions where the required annual reports have sometimes not appeared until several years have passed).

In this context, we call for the government's public commitment to the enactment of sufficient safeguards to match the array of new and existing powers.

⁵ See *R. v. Six Accused Persons*, [2008] B.C.J. No. 293 (S.C.) and *R. v. Riley*, [2008] O.J. No. 2887 (S.C.J.).

- 7 -

Support for this call can be found in recent U.S. and Canadian court decisions. In a unanimous decision of September 6, 2011 requiring the U.S. Department of Justice to publicly disclose information showing the government's use of cell phone location data in criminal prosecutions resulting in a guilty plea or a conviction, the United States Court of Appeals for the District of Columbia determined that:

The disclosure sought by the plaintiffs would inform ... ongoing public policy discussion by shedding light on the scope and effectiveness of cell phone tracking as a law enforcement tool. It would, for example, provide information about the kinds of crimes the government uses cell phone tracking data to investigate. As the plaintiffs note, with respect to wiretapping Congress has balanced privacy interests with law enforcement needs by permitting the government to use that technique for only the more serious offenses ... and the plaintiffs (and others) may decide to argue for similar legislation to govern cell phone tracking. Disclosure would also provide information regarding how often prosecutions against people who have been tracked are successful, thus shedding some light on the efficacy of the technique and whether pursuing it is worthwhile in light of the privacy implications.⁶

And, as indicated above, recent rulings of the Superior Courts of Ontario and British Columbia have determined that notice and reporting safeguards are constitutionally required with respect to intrusive surveillance powers, such as the power Parliament granted peace officers in section 184.4 of the *Criminal Code* (a power to conduct warrantless wiretapping in certain exceptional circumstances). For example, in *R. v. Six Accused Persons*, the B.C. Supreme Court determined that:

Although the Crown submits that in most cases where ... persons whose communications have been intercepted will receive *de facto* notification by way of the prosecution of the underlying offence, that submission fails to recognize that the communications of persons other than the alleged perpetrator may have been intercepted. It also fails to address situations where, for whatever reason, the police may have erred in their assessment of the need to intercept private communications, intercepted more communications than those to which they were lawfully entitled or over a longer period of time, or those that were intercepted under circumstances which did not result in a prosecution.

In any or all of those circumstances, the police would be answerable to no one. Further, the fact that there is no obligation to disclose surreptitious invasions of privacy to those persons whose communications have been intercepted removes an important safeguard to the potential abuse of power that can arise without accountability.

⁶ *American Civil Liberties Union v. United States*, United States Court of Appeals for the District of Columbia Circuit, September 6, 2011, No. 10-5159.

.../8

- 8 -

This case is illustrative of some of those concerns ... To this day, many of the persons whose communications were intercepted by the police are unlikely to know of that invasion of their privacy. That circumstance is exacerbated by the police having engaged in the automatic monitoring of all calls to the telephones they had identified as being appropriate for interception. Any discovery by third parties of the police having intercepted their private communications would be fortuitous.

Requirements to notify persons whose private communications have been intercepted of the fact of that interception afford an important constitutional and accountability safeguard to the potential abuse of state power in invading the privacy of its citizens.

The interception of private communications in exigent circumstances is not like situations of hot pursuit, entry into a dwelling place to respond to a 9-1-1 call, or searches incidental to arrest when public safety is engaged. In those circumstances, the person who has been the subject of a search will immediately be aware of both the circumstances and consequences of police action. The invasion of privacy by interception of private communications will, however, be undetectable, unknown and undiscoverable by those targeted unless the state seeks to rely on the results of its intentionally secretive activities in a subsequent prosecution.

I am accordingly satisfied that the failure of ... the [*Criminal Code*] to provide notification of surreptitious interception of private communications to those persons whose communications are intercepted is a serious impediment to the constitutional validity of s. 184.4.

.....

If the intention of Parliament in requiring the provision of [public] reports [enumerating resort to surveillance powers] is to oversee the frequency and circumstances of the interception of private communications by the police, the failure to provide a similar reporting requirement under s. 184.4 of the *Code* removes the potential for that oversight. As with the failure to require notification of those intercepted of the fact of an interception, the lack of any reporting requirement undermines both constitutionality and police accountability.⁷

Bearing all of the above in mind, and in addition to the adjustments we call for to Bills C-51 and C-52, we renew our call for the creation of an independent, arm's-length *Surveillance and Access Review Agency (SARA)*, with a legislative mandate to supervise state access to the highly sensitive personal information associated with digital communications and to report annually to Parliament and the public on the use of the surveillance and access powers.⁸

⁷ *R. v. Six Accused Persons*, [2008] B.C.J. No. 293 (S.C.)

⁸ For more information about the functions and duties we propose for *SARA*, please see our April 21, 2005 letter to the then Minister of Justice and Attorney General of Canada.

.../9

In establishing *SARA*, Parliament would require law enforcement and security agencies who obtain any communication-related data from TSPs to notify all of the individuals whose personal information is involved within one year of the information being obtained unless the individual cannot readily be identified or reasonably located, or notification would prejudice an ongoing investigation. Notification of all readily identifiable individuals would be required within five years of the information being obtained unless, on application to *SARA*, it is determined that the public interest in non-disclosure outweighs the right to notification.

In this context, TSPs should be required to publish annual reports on how many interception and access orders (and requests) they receive a year from which law enforcement and security agencies, in respect of how many individuals; and how many orders (and requests) result in the disclosure of personal information, and in respect of how many individuals.

In renewing the call for the creation of *SARA*, we acknowledge that the preparation and enactment of the necessary legislative framework will take time and that, in the meantime, the government may well decide to proceed with its plan to substantially reshape the state's capacity to conduct surveillance. To the extent that you are not prepared to redraft the Bills to ensure that the new surveillance powers are justified and that the necessary safeguards are in place before the regime comes into force, we strongly urge you to publicly commit to enact a *SARA Act* in tandem with the proposed surveillance and access regime, even as you move to amend the current legislative proposals to provide additional if limited safeguards on it coming into force, as further discussed below.

3) Even with Matching Oversight, the Proposed Powers Require Adjustment

Bill C-51, the *Investigative Powers for the 21st Century Act*, will amend the *Criminal Code*, giving "peace officers" and "public officers" new avenues to obtain access to information generated electronically. As such, a wide range of officers, extending well beyond police, will be empowered to:

- Issue preservation demands on their own say so with respect to a wide array of primarily corporate-held data in the course of investigating any offence, including on behalf of a foreign state, and impose any conditions in the demand that they consider appropriate, including conditions prohibiting the disclosure of its existence or some or all of its contents,
- Apply for new suspicion-based preservation and production orders to preserve and gain access to information about transmission, traffic, communication, tracking, transaction and financial data,
- Apply for new suspicion-based warrants to enable the remote live tracking of vehicles and other things,
- Apply for belief-based warrants to enable the remote live tracking of individuals by tracking the location of cell phones or other things they usually carry or wear, and
- Apply for non-disclosure/secretcy orders with respect to all of the above.

.../10

It is our view that, as a general rule, law enforcement access to data, particularly communications-related data, as well as the new tracking powers, should be subject to prior judicial scrutiny, limited to the investigation of serious crime, generally subject to higher belief rather than suspicion-based thresholds, and come with additional oversight and accountability-related safeguards.

In this context, I note that an August 22, 2011 U.S. District Court decision invites us to raise the question as to the constitutionality of the proposed suspicion-based, as well as belief-based, production order making powers.⁹ In this case, the U.S. government had asked the Court for “orders directing Verizon Wireless, a cell-phone service provider, to disclose recorded information of cell-site-location records for one of its customers pursuant ... to the *Stored Communications Act* or ‘SCA’).” The proposed order sought stored, historical cell-site-location records tied to a period in excess of 113 days. On its face, the *SCA* provides that such an order “may be issued by ... a court of competent jurisdiction ... only if the governmental entity offers specific and articulable facts showing that there are *reasonable grounds to believe* that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.” (Emphasis added.) The Court determined that “the Fourth Amendment to the United States Constitution requires a warrant and a showing of probable cause before the Government may obtain the cell-site-location records requested here.”

As the Court clearly understood, the problem with these kinds of production orders is their implication for the privacy of society at large and, in my view, the concerns expressed by the Court with respect to Americans apply equally with respect to Canadians:

The vast majority of Americans own cell phones. Many Americans have abandoned land line phones entirely, and use cell phones for all telephonic communications. Typically people carry these phones at all times: at work, in the car, during travel, and at home. For many Americans, there is no time in the day when they are more than a few feet away from their cell phones.

Cell phones work by communicating with cell-sites operated by cell-phone service providers. Each cell-site operates at a certain location and covers a certain range of distance. The number of cell-sites that must be placed within a particular area, and thus the distance between cell-sites, is determined by several factors, including population density.

If a user’s cell phone has communicated with a particular cell-site, this strongly suggests that the user has physically been within the particular cell-site’s geographical range. By technical and practical necessity, cell-phone service providers keep historical records of which cell-sites each of their users’ cell phones have communicated.

⁹ *In the matter of an application of the United States of America for an Order authorizing the release of historical cell-site information* No. 10-MC-897, United States District Court, E.D. New York (August 22, 2011).

- 11 -

The implication of these facts is that cellular service providers have records of the geographic location of almost every American at almost every time of day and night. And under current statutes and law enforcement practices, these records can be obtained without a search warrant and its requisite showing of probable cause.

What does this mean for ordinary Americans? That at all times, our physical movements are being monitored and recorded, and once the Government can make a showing of less-than-probable-cause, it may obtain these records of our movements, study the map our lives, and learn the many things we reveal about ourselves through our physical presence.

In the same vein, in the *Maynard* case now pending before the U.S. Supreme Court, the reasoning of the United States Court of Appeals for the District of Columbia provokes questions as to the constitutionality of the proposed suspicion-based, as well as belief-based, *tracking* warrants. As the Appeal Court found in *Maynard*, "prolonged GPS monitoring [of a person's vehicle travelling on public roads] defeats an expectation of privacy that our society recognizes as reasonable" and must comply with Fourth Amendment standards.

The Court's holding was echoed as recently as September 21, 2011 in a report issued by the *Liberty and Security Committee* of the U.S. *Constitution Project*. This bi-partisan committee, whose members include two former members of Congress, former FBI director William Sessions, a former U.S. Court of Appeals judge and a former chair of the American Conservative Union, concludes that "when powerful tracking technologies to conduct pervasive surveillance are paired with [a computer's] analytic capability and a digital database, such monitoring can violate an individual's reasonable expectation of privacy even in a public place."

The Committee recommends that, if the U.S. Supreme Court does not adopt the proper approach in the *Maynard* case, Congress should do so by enacting legislation requiring court warrants for any location tracking lasting more than 24 hours.¹⁰

Consistent with these developments, in my view, it is essential that more stringent conditions precedent be enacted in relation to the proposed surveillance and access powers. The use of production orders and tracking warrants should be confined to investigations in respect of the list of serious offences in section 183 of the *Criminal Code*. Before issuing such orders or warrants, a superior court judge ought to be satisfied that:

- There are reasonable and probable grounds to believe that an offence under section 183 of the *Criminal Code* has been or is being committed,
- Other less intrusive investigative methods are likely to prove impracticable,

¹⁰ See the Liberty and Security Committee September 21st, 2011 *Statement on Location Tracking* at <http://www.constitutionproject.org/pdf/LocationTrackingReport.pdf>.

- Measures will be taken to safeguard the privacy of the personal information obtained, particularly of non-suspects, and
- The intrusion is otherwise in the best interests of the administration of justice.

As indicated, Bill C-51 also proposes to create a new set of powers that police could invoke to require data managers to locate and hold personal information in documents or databanks. Government has argued that these preservation powers are necessary to support the production order powers discussed above. In our view, any power to issue a preservation demand or order should be confined to the same list of serious offences in section 183 of the *Criminal Code*.

In addition, in order to address the risk to accountability that non-disclosure or secrecy orders entail, we recommend that all those whose personal information is obtained under a surveillance and access regime should be entitled to notification at the appropriate time. And, in accord with our *SARA*-related recommendations, state use of these powers and access to this personal information should be superintended and reviewed by an independent agency.

It is also noteworthy that in introducing sections 487.0195(1) and (2) to the *Criminal Code*, Bill C-51 provides broad immunity from “any criminal or civil liability” to any person who voluntarily preserves data or provides a document to an officer. The person is no longer required to show that he or she acted on reasonable grounds *per* the operation of what is now section 487.014 with section 25 of the *Criminal Code*. The person need only show that his or her cooperation was not “prohibited by law.” In our view, individuals and entities responsible for safeguarding personal information of members of the public must act reasonably before they should be entitled to such immunity. A reasonableness standard provides volunteers with significant protection while helping to rule out the possibility that, for example, malicious or incompetent decision makers will enjoy undeserved immunity.

Accordingly, section 487.0195(2) should be amended to provide that:

A person who preserves data or provides a document in the circumstances described in subsection (1) does not incur any criminal or civil liability for doing so if he or she acted reasonably in the circumstances.

Bill C-50, the *Improving Access to Investigative Tools for Serious Crimes Act*, will amend the *Criminal Code*, first by providing that if a wiretap authorization is granted under Part VI, the judge may at the same time issue one or more Bill C-51-related warrants or orders that relate to the investigation in respect of which the wiretap authorization is given. That is, in obtaining a wiretap warrant, police may also contemporaneously obtain companion production orders and tracking warrants, all from a single judge. Rules respecting secrecy and confidentiality that apply in respect of a wiretap authorization will also apply in respect of a request for a related warrant or order. In addition, the Bill will permit a peace officer or a public officer to install and make use of a number recorder without a warrant in exigent circumstances. The Bill will also extend to one year the maximum period of validity of a warrant for a tracking device and a number recorder if the warrant is issued in respect of a terrorism offence or an offence relating to a criminal organization (the maximum is now 60 days).

The critical development brought forward in Bill C-50 is that the efficiencies it may purchase in streamlining the conduct of judicially authorized state surveillance and access may come at some cost to the rigour of prior judicial scrutiny. In some cases, a single judge hearing a multitude of inter-related applications may be better informed about the extent of the overarching surveillance employed. At the same time, the demands on judges are likely to grow. In the context of what are necessarily *ex parte* and *in camera* proceedings, there will be an increased risk that a greater degree of intrusive surveillance and access will be granted in cases where it is not warranted. While we do not oppose Bill C-50 *per se*, its enactment will likely intensify the effect of the new surveillance regime. Such intensification increases the need for the adoption of matching safeguards under a *SARA Act*.

4) Surveillance Must Not Undercut the Future of Freedom, Innovation and Privacy

In addition to the controversial plan to provide law enforcement with warrantless access to subscriber information (discussed in section 5 below), the *Electronic Communications Act* sets in motion a fundamental change to the way communication services are regulated. It does so by entrenching the power of security officials to require TSPs to:

- Build in and continuously maintain a wide array of yet to be specified interception capabilities into all their networks, systems and software for the purpose of allowing authorized agencies to intercept, isolate and accurately correlate multiple communications per court orders,
- Notify law enforcement and CSIS officials regarding changes to state provided equipment or systems where those changes are likely to reduce interception capability;
- Assist designated persons who will have warrantless access to TSP facilities, systems, documents and information to test, inspect, and access TSP facilities, services and systems for regulatory purposes,
- Provide prescribed specialized telecommunications support to CSIS and law enforcement agencies,
- Submit lists of TSP personnel to CSIS and/or the RCMP for the purposes of conducting security assessments of employees who may assist in the interception of communications, and
- Comply with prescribed confidentiality and security measures.¹¹

The *Electronic Communications Act* will also establish numerous offences and violations and subject TSPs, their officers, directors, and employees to prosecution and fines for failing to comply with obligations, including those relating to systems requirements.

¹¹ Note that, to date, security officials have been able to impose a similar framework largely outside Parliamentary scrutiny through, for example, the Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications, and Conditions of Licence for New Cellular and PCS Licences issued by the Minister of Industry under the *Radiocommunication Act* (see <http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf09251.html>).

Each additional day in breach of the statute will add to the count of violations and increase the exposure of TSPs, their officers, directors, and employees to fines of up to \$50,000 per offence for an individual and \$250,000 for a corporation. The *Electronic Communications Act* will allow the state to seek a court injunction ordering a TSP to cease operating a transmission apparatus, or to refrain from acquiring, installing or operating new software, if the TSP is contravening or likely to contravene interception requirements.

It is also noteworthy that the *Electronic Communications Act* does not address the financial and commercial implications of these proposals, either to businesses, consumers, or taxpayers. It only authorizes the payment of some monies to compensate TSPs in relation to: (i) compliance with a Ministerial order to provide interception capabilities additional to those prescribed; (ii) the provision of subscriber information; and (iii) the provision of certain specialized telecommunications support. Reports about the cost of related proposals in the U.S. and the U.K. warrant careful consideration in Canada.

In October of 2010, it was reported that, in response to the Obama administration's intention to submit comparable surveillance legislation, American TSPs are "likely to object to increased government intervention in the design or launch of services. Such a change ... could have major repercussions for industry innovation, costs and competitiveness."¹²

In the U.K., a related though more intrusive data retention and "Interception Modernization Program" was being considered until it was abandoned by the British government in late 2009 because of concerns about cost, controversy and feasibility. Prior to this, it was reported that development costs will be high (2 to 13 billion pounds). "The bulk of the costs will be incurred by [TSPs]. The most ignored cost comes in the form of opportunity costs as engineers will be tasked to develop this [surveillance] solution instead of developing their core business, *i.e.* new ways to enhance the networks for advancing consumer and business interests."¹³

None of these immediate financial costs would necessarily translate into privacy issues *per se* if it were not for the fact that the *Electronic Communications Act* risks causing additional marketplace distortions by effectively prohibiting the use and development of any systems or software that might impair a TSP's capacity to facilitate simultaneous multiple intercepts. While the goal of facilitating compliance with court ordered surveillance is valid, there is a significant risk that in implementing this legislation, the authorities will impede the development and use of new communications technologies and services, particularly, for example, privacy enhancing technologies and services such as those that provide for encryption.

In this regard, the *Electronic Communications Act* requires that a TSP must "use the means in its control" to provide an intercepted communication "in the same form as it was before the communication was treated by the service provider" by way of encoding, compression, or encryption. A TSP is not required to make the form of an intercepted communication the same as it was before the communication was treated if it would be required to develop or acquire new

¹² "Officials Push to Bolster Law on Wiretapping", Charlie Savage, New York Times, October 18, 2010.

¹³ London School of Economics, *Briefing on the Interception Modernisation Programme*, June 2009, p. 44-45.

- 15 -

decryption techniques or tools. The legislation appears to allow companies like Research in Motion to continue to provide existing encryption protected communication services. It remains to be seen what the future holds for new companies and new strong encryption techniques and services in the field of communications. For example, there is a risk that the *Electronic Communications Act* will set the stage for rules requiring back-door state access to encryption services.

It is evident that many of the critical details flowing from the *Electronic Communications Act* will be left to policies, procedures, regulations and evolving relationships between TSPs and the state. In passing so many significant public policy decisions on to security-oriented officials, Parliamentarians and the public risk being left out of the decision-making process and Canadians risk seeing TSPs transformed into agents of the state. This represents a significant and needless risk to a free and open society.

We only have to look to recent U.S. history to consider the implications. Many will now be familiar with reports of the secretive and controversial assistance that major telecommunications carriers provided the National Security Agency in the conduct of warrantless eavesdropping on international calls by suspected terrorists after 9/11. As recognized by U.S. courts, such surveillance has the potential to expose "journalistic sources, witnesses, experts, foreign government officials, and victims of human rights abuses located outside the United States" to "violence and retaliation by their own governments, non-state actors, and the U.S. government."¹⁴

While the *Electronic Communications Act* will be subject to a form of Parliamentary review five years out, in the meantime, if passed, it will substantially alter the design and operation of communication systems, the role and function of TSPs, their ability to be transparent, and the relationship between citizens, TSPs and the state.

A comprehensive and public cost benefit analysis should *precede* rather than follow the making of so many significant public policy decisions. Before imposing the kind of interception capacity regime the *Electronic Communications Act* would impose on TSPs, Parliament should ensure that such a capacity regime will be proportionate and designed to ensure not only appropriate surveillance capacity but also necessary competitiveness and privacy.

It follows that the Parliamentary committee eventually mandated to consider the kinds of proposals in the *Electronic Communications Act* should be adequately resourced to ensure that civil society, as well as industry, has a full opportunity to provide substantial input.

In addition, the *Electronic Communications Act* should be amended to require that all interception-related capacity requirements be *publicly* vetted for their impact on privacy and competitiveness *before* they are imposed (in the future, *SARA* should have a role to play in reporting on the impact of capacity-related requirements). Such requirements should be

¹⁴ *Amnesty Int'l USA et al. v. Clapper et al.*, United States Court of Appeals for the Second Circuit, September 21st, 2011, 09-4112-cv, at pages 8-9 of Circuit Judge Lynch's decision, quoting from *Amnesty Int'l USA v. Clapper*, 638 F.3d 118 (2d Cir. 2011).

.../16

provided for in the form of draft regulations which would only come into force after a vote by Parliament to approve them as a whole.

5) Warrantless Access to Subscriber Information Must Be Withdrawn

In addition to providing the state with substantial control over the design and operation of TSP systems, the *Electronic Communications Act* will also provide law enforcement and CSIS officials with *warrantless* access to subscriber information for the purposes of performing *any* of their duties or functions. Subscriber information includes a named individual's IP address or mobile ID number, or the name and contact information of a subscriber associated with an IP address or mobile ID number.

The *Electronic Communications Act* provides for attenuated *post facto* review of warrantless access to subscriber information. In doing so, it relies on provincial and territorial privacy commissioners to: (i) conduct audits to assess local and provincial police compliance with provisions of the statute empowering the collection and use of subscriber information; and (ii) review police reports generated to the extent that police decide that something has occurred with respect to their own exercise of these access powers that, in their opinion, ought to be brought to the attention of the responsible provincial minister (in Ontario, the attorney general).

Under section 20(6) of the legislation, the Privacy Commissioner of Canada must provide Parliament with an annual report identifying the provincial and territorial privacy commissioners who may receive any such opinion-based reports and the powers that they have to conduct section 20 compliance audits.

Like a number of other provincial and territorial privacy commissioners, I lack the necessary powers. In particular, under Ontario's privacy statutes, I do not have any audit powers. Even those privacy commissioners with sufficient powers are likely to need additional resources in order to adequately perform the legislative duties imposed under section 20 of the *Electronic Communications Act*.

In a letter of March 9, 2011 signed by all the federal, provincial and territorial privacy commissioners, we joined our colleagues in calling on the federal government to commit to working with provincial and territorial governments to ensure that all of our offices have sufficient powers and resources should the *Electronic Communications Act* be enacted. It does not appear that any such commitment has been forthcoming.

Quite apart from the constitutional issues raised by the enactment of a regime of warrantless access, it is noteworthy that in some circumstances, aspects of *post facto* oversight of communications-related surveillance powers have been found by Superior Courts to be constitutionally required (see, for example *R. v. Six Accused Persons*, [2008] B.C.J. No. 293 and *R. v. Riley*, [2008] O.J. No. 2887). In the absence of the necessary provincial and territorial powers and resources, the *Electronic Communications Act's* reliance on provincial and territorial privacy commissioners is untenable. In addition, the audit duties to be imposed on provincial and territorial privacy commissioners under section 20 may raise division of powers problems.

.../17

- 17 -

It remains our view that the *Electronic Communications Act* should be amended to require that provisions setting out TSP obligations concerning "subscriber information" should be deleted and replaced with a court supervised regime.

"Subscriber information" is personal information. To date, all individual customers enjoy the legal right to insist that, subject to narrowly defined exceptions, their subscriber information remains private and confidential. The law currently provides for warrant procedures, expedited tele-warrants, and an organization's special exercise of discretion to disclose personal information to law enforcement without an individual's consent, for example, in aid of an Internet-related child pornography investigation, or in comparable exigent-like circumstances. Granting law enforcement and intelligence officials an almost unfettered power to issue their own administrative "warrants" for the purposes of performing *any* of their duties or functions is a substantial departure from the legal and constitutional framework in Canada. Such a departure requires extraordinary justification and a substantial framework for accountability.

Consistent with our earlier comments, law enforcement and security agency access to information linking subscribers to devices (and *vice versa*) should generally be subject to prior judicial scrutiny accompanied by the appropriate checks and balances. Before issuing an order requiring the disclosure of subscriber information, a judge ought to be satisfied that:

- There are reasonable and probable grounds to believe that an offence under section 183 of the *Criminal Code* has been or is being committed,
- Measures will be taken to safeguard the privacy of the personal information obtained, particularly of any non-suspects, and
- The intrusion is otherwise in the best interests of the administration of justice.

In the alternative, if Parliament is determined to allow warrantless access to subscriber information, the legislative safeguards in section 20 of the *Electronic Communications Act* should be strengthened so that they provide a much greater degree of *post facto* oversight. In particular:

- The power to demand warrantless access to subscriber information should be narrowed to only apply in circumstances where access is necessary to the investigation of a specific and defined category of serious crime, for example, sexual offences involving children and minors, or to prevent or eliminate a significant and imminent risk of serious bodily harm.
- The "consistent use" limitation regarding subscriber information collected by law enforcement and security agencies should be strengthened. A use should only be considered as consistent if a reasonable person might reasonably have expected such a use.

.../18

- 18 -

- Law enforcement and security agencies should be required to securely destroy information that is provided in response to a subscriber information request one year after the individual has been notified of its collection, or once retention of the information is no longer necessary for the purpose for which the information was obtained, or for a use consistent with that purpose, whichever is later.
- The requirement that law enforcement and security agencies must report to attorneys general and privacy commissioners should be strengthened. Agencies should be expressly required to report any collection, use or retention practices that do not appear to be necessary and proportionate in relation to the duty or function for which they were originally obtained.
- In reporting to Parliament on the adequacy of audit and investigation powers available to provincial and territorial privacy commissioners, the Privacy Commissioner should also report on whether those commissioners consider themselves to have adequate resources to conduct the necessary audits and reviews.
- If, after consulting with a provincial or territorial commissioner, the Privacy Commissioner reports that her colleague does not have substantially similar powers, the subscriber information powers available to police services within that jurisdiction should *automatically* lapse until the Privacy Commissioner reports back that the provincial or territorial commissioner has been provided with those powers.

To the extent that Parliament chooses to rely on provincial and territorial privacy commissioners to perform *post facto* review of warrantless access to subscriber information, it follows that the federal government must commit to working with provincial and territorial governments to ensure that all of the relevant privacy commissioners have sufficient powers and resources. In this regard, please note that I have written two letters to Ontario's Attorney General, asking that the Ontario government play its part in these important law reform and oversight-related issues. Copies of those letters are attached.

Conclusion

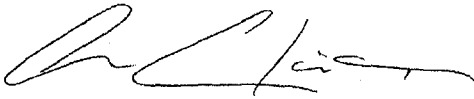
The surveillance regime being put forward is aimed at capturing the full range of content, communication and traffic data associated with digital communications. As communication services continue to evolve, the legislation will empower the state to develop, update and enforce regulations directly aimed at shaping the technological capacities of telecommunication services so as to ensure that Web 2.0, 3.0 etc. communications can be readily intercepted, isolated and accurately correlated. In this context, it is reasonable to foresee that it will be much easier for the state to subject more individuals, including innocent individuals, to unwanted surveillance and scrutiny.

.../19

- 19 -

This debate is not about maintaining the state's surveillance capabilities, but trying to determine the proper balance in the evolving information age. In the face of so many significant changes, with so much at stake, and with so much left to regulation and implementation by policy, we are concerned that the public, Parliament and industry will be hard pressed to keep abreast of the technological challenges, the financial costs, and the invasiveness of an *expanding surveillance regime*. It is essential that Parliament and the public be well informed on technological, legal, regulatory and financial issues. The implications for privacy and other human rights must also be fully addressed, by providing for the necessary transparency, accountability and oversight. No less than the future of privacy – the future of freedom, is at stake.

Yours sincerely,



Ann Cavoukian, Ph.D.
Commissioner

Enclosures (2)

c: The Honourable John Gerretsen, Attorney General of Ontario
William Baker, Deputy Minister, Public Safety Canada
Myles Kirvan, Deputy Minister of Justice & Deputy Attorney General of Canada
Murray Segal, Deputy Attorney General of Ontario



Information and Privacy
Commissioner/Ontario
Commissaire à l'information
et à la protection de la vie privée/Ontario

VIA EMAIL AND COURIER

October 24, 2011

The Honourable John Gerretsen
Attorney General of Ontario
Ministry of the Attorney General
McMurtry-Scott Building
720 Bay Street, 11th Floor
Toronto, ON M7A 2S9

Dear Minister Gerretsen:

I am writing to congratulate you on your appointment as the Attorney General of Ontario. While I have enjoyed a good working relationship with you in your previous Ministry, I look forward to working with you in your new capacity. In this regard, I think we may both benefit from an opportunity to meet briefly in person, perhaps early in the new year. If you are interested, my office will be in contact with yours to confirm a date and time.

In addition, I attach a copy of my September 23rd, 2011 letter to Minister Bentley, with whom my office also enjoyed a productive relationship, regarding section 20 of Bill C-52, the *Investigating and Preventing Criminal Electronic Communications Act (ECA)*. While this and two other related bills died on the Order Paper at the end of Parliament, I understand that the federal government intends to re-introduce all three shortly, in essentially the same format.

Over the last few weeks, public dismay about the likely re-introduction of Bills C-50, C-51, and C-52 has been growing. Many of the grave concerns that I and other privacy commissioners have had about these proposals were reflected in the October 22nd, 2011 article in the *National Post, Laws for 21st century: A guide to Canada's proposed cyber investigation bills* (copy attached).

Read together, their enactment would substantially diminish the privacy rights of Canadians. They would do so by enhancing the capacity of the state to conduct surveillance, as well as access private information, while reducing the frequency and vigour of judicial scrutiny, thus making it easier for the state to subject more individuals to expanded surveillance and scrutiny.

My concerns about these legislative proposals can be summarized as follows:

- The proposed surveillance powers come at the expense of the necessary privacy protective constitutional balance. In order to maintain that crucial balance, the federal government must be persuaded to acknowledge the sensitivity of traffic data, stored data, and tracking data and to re-draft the bills accordingly.



2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

.../2
Tel: 416-326-3333
1-800-387-0073
Fax/Télééc: 416-325-9195
TTY: 416-325-7539
www.ipc.on.ca

000394

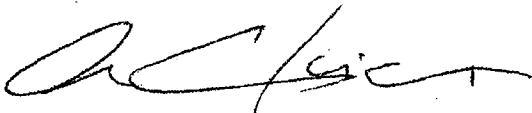
- 2 -

- Intrusive proposals require matching legislative safeguards. The courts, affected individuals, future Parliaments, and the public must be well informed about the scope, effectiveness, and deleterious effects of intrusive powers. If the federal government pushes ahead with expansive new surveillance powers, I hope you will join me in urging the federal government to publically commit to enacting the necessary oversight legislation, in tandem.
- Even with matching oversight, the proposed surveillance and access powers require more stringent conditions precedent.
- Entrenching a mandatory surveillance capacity regime on the public and its telecommunications service providers (TSP) must not go forward without adequate safeguards to protect the future of privacy and freedom; a comprehensive cost-benefit analysis, made publicly available, should precede rather than follow the making of so many significant public policy decisions. Public Parliamentary hearings should also be scheduled to ensure that civil society, as well as industry, have a full opportunity to provide substantial input on all of the bills, including the *ECA*.
- The proposal for warrantless access to subscriber information is untenable and should be totally withdrawn. It remains our view that the *ECA* should be amended to require that the provisions setting out TSP obligations concerning "subscriber information" be deleted and replaced with a court supervised regime.

While I continue to have the specific concerns about the focused legal and fiscal issues outlined in my September 23rd letter, I believe it is increasingly important for you to be aware of the *overarching* surveillance and access proposal and the serious implications it has for the privacy rights of the residents of Ontario as a whole.

Once again, congratulations on your appointment. I wish you every success in the important work ahead.

Sincerely yours,



Ann Cavoukian, Ph.D.
Commissioner

Enclosure



Information and Privacy
Commissioner of Ontario
Commissaire à l'information
et à la protection de la vie privée de l'Ontario

September 23, 2011

VIA EMAIL AND LETTER MAIL

The Honourable Chris Bentley
Attorney General of Ontario
Ministry of the Attorney General
McMurtry-Scott Building
720 Bay Street, 11th Floor
Toronto, ON
M7A 2S9

Dear Minister Bentley:

I am writing you in relation to a single aspect of the federal government's anticipated package of surveillance-related legislation. My concerns focus on the legal and fiscal factors likely to undermine my capacity to fulfil the role the federal government purports to assign to my office under section 20 of Bill C-52, the *Investigating and Preventing Criminal Electronic Communications Act* (hereafter referred to as the *Electronic Communications Act* or *ECA*). While this bill died on the Order Paper at the end of the last Parliament, I understand that the federal government may re-introduce it in essentially the same form shortly.

In addition to providing the state with substantial control over the design and operation of "telecommunication service providers" (TSP) systems, the *Electronic Communications Act* would provide law enforcement and CSIS officials with warrantless access to *subscriber information* for the purposes of performing any of their duties or functions. *Subscriber information* includes a named individual's IP address or mobile ID number or the name and contact information of a subscriber associated with an IP address or mobile ID number.

Access to TSP-held *subscriber information* will empower police to link specific communication devices with particular individuals, as well as to monitor a wide range of their communications and activities in cyberspace. Since this power would be available for the purposes of performing *any* police duties or functions, the potential benefits and risks will be comparably wide ranging.

Section 20 of the *ECA* provides for attenuated *post facto* review of warrantless access to subscriber information. In doing so, it relies on provincial and territorial privacy commissioners and ombudsmen ("public officers" or "privacy officers") to: (i) conduct audits to assess local and provincial police compliance with provisions of the Bill that broadly empower the collection and use of subscriber information; and (ii) review police reports generated after police determine that something has occurred with respect to their own exercise of these access powers that, in their opinion, ought to be brought to the attention of the responsible provincial minister (in Ontario, the Attorney General).

.../2



Legal Services Department
2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

Services juridiques
2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel: 416-326-3333
1-800-387-0073
Fax/Télé: 416-325-9186
TTY: 416-325-7539
www.ipc.on.ca

000396

- 2 -

Under section 20(6) of the *ECA*, the Privacy Commissioner of Canada must provide Parliament with an annual report identifying the provincial privacy officers who may receive any such opinion-based reports and the powers that they have to conduct section 20 compliance audits.

In my case, I lack the powers necessary to fulfill the proposed duties. In fact, under our home statutes, I do not have any audit powers. This may be the case for other provincial and territorial officers. This concern was reflected in a letter of March 9, 2011 signed by all the federal, provincial and territorial privacy officers. In that letter, we joined our colleagues in calling on the federal government to commit to working with provincial and territorial governments to ensure that all of our offices have sufficient powers and resources should the *Electronic Communications Act* be enacted. It does not appear that any such commitment has been forthcoming.

As I am sure you will agree, under these circumstances, the federal government's approach to oversight is clearly untenable. Quite apart from the constitutional issues raised by the enactment of a regime of warrantless access, it is noteworthy that in some circumstances, aspects of *post facto* oversight of communications-related surveillance powers have been found to be constitutionally required (see, for example *R. v. Six Accused Persons*, [2008] B.C.J. No. 293] and *R. v. Riley*, [2008] O.J. No. 2887). In addition, the audit duties to be imposed on my office under section 20 may raise division of powers problems.

Finally, I note that I would lack the necessary fiscal and human resources required to adequately perform the legislative duties imposed under the *Electronic Communications Act*.

While it continues to be our view that the *Electronic Communications Act* should be amended to ensure that police access to *subscriber information* is subject to a system of prior judicial authorization, it appears likely that the federal government will move ahead with a system of warrantless access and attenuated *post facto* review.

In this context, I wanted to alert you to the federal government's apparent failure to account for these significant problems and to urge you to raise these matters with your federal counterparts. Should they insist on proceeding in this direction, you may be faced with having to address uninvited legislative, fiscal, and constitutional issues.

Please do not hesitate to contact me if you wish to discuss these matters further.

Sincerely yours,



Ann Cavoukian, Ph.D.
Commissioner

cc: Murray Segal, Deputy Minister

Veilleux, Martine

From: Commissioner IPC <Commissioner.IPC@ipc.on.ca>
Sent: Monday, October 31, 2011 12:11 PM
To: 'vic.toews@parl.gc.ca'; 'Nichor@parl.gc.ca'
Cc: 'john.gerretsen@ontario.ca'; 'murray.segal@ontario.ca'; 'johanne.rousseau@justice.gc.ca'; Baker, William V.; Ken Anderson; Brian Beamish
Subject: 383494: Privacy Implications of Expanded Surveillance - Letter from Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario
Attachments: 2011 October 31 Letter to Ministers Toews and Nicholson Lawful Access.pdf
Importance: High
Follow Up Flag: Follow up
Flag Status: Completed

Dear Ministers,

Please find attached a letter from Commissioner Cavoukian regarding privacy implications of expanded surveillance.

Regards,

Debra Adair
Administrative Assistant to Dr. Ann Cavoukian, Commissioner
Office of the Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Office: 416-326-3936 (direct)
Fax: 416-212-6523 (office fax)
TTY: 416-325-7539



www.privacybydesign.ca

You can also follow Privacy by Design on Twitter [@embedprivacy](https://twitter.com/embedprivacy)



Information and Privacy
Commissioner of Ontario
Commissaire à l'information
et à la protection de la vie privée de l'Ontario

October 31, 2011

VIA ELECTRONIC MAIL AND COURIER

The Honourable Vic Toews
Minister of Public Safety
269 Laurier Avenue West
Ottawa, Canada
K1A 0P8

The Honourable Robert Nicholson
Minister of Justice and Attorney General of Canada
284 Wellington Street
Ottawa, Ontario
K1A 0H8

Dear Ministers:

Introduction

As the Information and Privacy Commissioner of Ontario, I felt compelled to write to you today regarding the federal government's insistence on enacting a highly intrusive surveillance regime. I do so in full support of Canada's Privacy Commissioner Stoddart and the open letter she sent to Minister Toews on October 26th.

At the outset, please note that my mandate includes commenting on developments that affect the personal privacy of Ontarians, and overseeing law enforcement compliance with privacy legislation in Ontario. The proposed surveillance regime will have a substantial impact on the privacy rights of Ontarians, law enforcement functions, and the role of my office.

Media reports referring to Minister Toews' rejection of Commissioner Stoddart's concerns and quoting his defence of the regime suggest that the government will re-introduce Bills C-50, C-51, and C-52 ("the Bills") in essentially the same form in which they appeared in the last Parliament. In my view, that would be highly regrettable for the people of Ontario and Canada. I am writing this open letter to outline my specific concerns and concrete recommendations.

I have first summarized the privacy concerns identified by my office into five categories, followed by an in-depth discussion of each.

.../2



2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel: 416-326-3333
1-800-387-0073
Fax/Télé: 416-325-9188
TTY: 416-325-7539
www.ipc.on.ca

000399

- 3 -

1) New Powers Must Not Come at the Expense of the Constitutional Framework

In a steady stream of communiqués dating back almost a decade and spanning 2002, 2005, 2007, 2009, and 2011, our office has cautioned against taking a legislative approach to new surveillance powers that undermines the judicially supervised rules and procedures which secure our shared rights to privacy, freedom and security of the person. Two of these were in joint communiqués led by the Privacy Commissioner of Canada, and signed by all the provincial and territorial privacy commissioners and ombudsmen (“privacy commissioners”).¹

Together, they accurately reflect the general nature of many of our current concerns and recommendations. (We also urge you to carefully consider the federal Privacy Commissioner’s November 2010 publication *A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century*.)

The concerns voiced by Canada’s privacy commissioners have been echoed by legal and academic experts specializing in technology, privacy and the law and, most importantly, by thousands of concerned Canadians who wish to have both effective law enforcement *and* strong privacy protections.

In this context, there can be little doubt that the most recent iteration of the government’s approach to expansive surveillance legislation has significant implications for personal privacy, state powers, and the longstanding constitutional compromise between the two, as well as for the oversight functions of courts and privacy commissioners, and the future of innovation, costs and competitiveness in the communications and technology fields.

The fact that the government appears to be committed to limiting real-time surveillance of private communications including in-transit e-mail under the “wiretapping” rules set out in Part VI of the *Criminal Code* is welcome news. We also welcome the absence of any public call for the creation of data retention rules with respect to subscribers and their day-to-day use of the new technologies. No such retention rules should be countenanced.

At the same time, we believe that critical elements of the proposed legislative regime suggest that the government misconceives how Canadians interact with new communications technologies and significantly underestimates the sensitivity of the personal information involved. The concomitant risks to privacy and other fundamental rights are significant.

¹ Copies of these five communiqués are available at:

December 20, 2002 - <http://www.ipc.on.ca/english/Resources/Reports-and-Submissions/Reports-and-Submissions-Summary/?id=114>; April 21, 2005 - <http://www.ipc.on.ca/english/Resources/Reports-and-Submissions/Reports-and-Submissions-Summary/?id=105>; October 10, 2007 - <http://www.ipc.on.ca/english/Resources/Reports-and-Submissions/Reports-and-Submissions-Summary/?id=662>; September 9-10, 2009 - http://www.priv.gc.ca/media/nr-c/2009/res_090910_e.cfm; and March 9, 2011 - http://www.priv.gc.ca/media/nr-c/2011/let_110309_e.cfm.

.../4

- 4 -

Why? Because new surveillance powers leverage new and still evolving technologies. As a result, they significantly *increase* rather than merely maintain the state's surveillance capacity. Accordingly, attempts to frame the public debate in terms of maintaining capacity are misleading:

The ways in which we communicate with each other have undergone such enormous changes that it is entirely fanciful to say that there are simple equivalents in the Internet and broader digital domain to the communications surveillance techniques used for conventional voice-based telephones. There are many new types of communication available between individuals, but nearly all of these are in forms that are very easily computer-readable and therefore capable of complex analysis by computers. The range of tools available to law enforcement to track and link activity and database content is now vast and growing all the time. The debate is thus not about maintenance of capability but trying to determine a proper balance in new circumstances.²

In this context, the legal distinction traditionally drawn between the content of a private communication such as is exchanged during a telephone call or via e-mail and the associated *traffic* data is being overtaken by social, economic and technological developments. What we refer to as traffic data has evolved and it will continue to do so. Certainly, it is no longer confined to a list of phone numbers obtained by a dial recorder or rows of text on a telephone bill.

It extends digitally to link and trace the ongoing interactions of networks of users through unique identifying device numbers *vis-à-vis* their location in time, their location on and along the ground, their activity and interactivity within the Internet, and their relatedness within and across communities. The resulting digital trails are routinely retained by service providers and various third parties for weeks, months or even years. These trails paint a detailed and evolving picture that reflects on who we are.

Furthermore, there are strong indications that law enforcement's appetite for the surveillance of live telephone communications is being dwarfed by their interest in accessing the private content in the mass of digital trails created every time an individual sends a message, surfs the Internet, e-banks or simply carries a 3G enabled device.³ Computer facilitated analysis of this data can readily reveal the interwoven layers of core biographical information that animate communications data, particularly where the scrutiny extends for a significant period of time. As recognized by the United States Court of Appeals for the District of Columbia in a Fourth Amendment GPS vehicle tracking case being heard by the U.S. Supreme Court on November 8, 2011:

² London School of Economics, *Briefing on the Interception Modernisation Programme*, June 2009, p. 6.

³ See "The Law Enforcement Surveillance Reporting Gap" by Christopher Soghoian, Indiana University Bloomington - Center for Applied Cybersecurity Research, April 10, 2011.

.../5

- 5 -

Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynaecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups — and not just one such fact about a person, but all such facts.⁴

Properly supervised, surveillance powers can be invaluable to law enforcement. However, it is equally true that where individuals are subject to unwarranted suspicions, evidence is poorly handled, or erroneous conclusions are hastily drawn, the consequences for innocent individuals can be devastating. Recent national security-related investigations make this all too clear (e.g., Maher Arar).

While we continue to support the vital law enforcement interest in pursuing electronic evidence and intelligence about serious wrongdoing, we also urge the government to ensure that any search, seizure, or surveillance of personal communications be subject to the most rigorous oversight. The constitutional values at stake demand such safeguards.

On the basis of all the above, we reject the Bills' implicit claim that the so-called non-content data elements associated with new communication devices and services are of significantly lesser constitutional significance. Safeguards comparable to those necessary to properly regulate the wiretapping of a rotary phone are required with respect to 21st century communications, including, but not limited to, rigorous prior judicial scrutiny.

2) Intrusive Proposals Require Essential Matching Legislative Safeguards

Read together, the legislative proposals substantially diminish the privacy rights of Canadians. They do so by enhancing the capacity of the state to conduct surveillance, as well as access private information, while *reducing the frequency and vigour of judicial scrutiny*, thus making it easier for the state to subject more individuals to surveillance and scrutiny.

Are the current processes that provide for oversight of surveillance-related powers sufficient to keep pace with the proposed expansion of state power? With the anticipated re-introduction of the Bills, Canadians are being asked to rely on oversight regimes designed decades ago to provide sufficient safeguards for the protection of our fundamental rights and freedoms today.

⁴ *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), cert. granted, *United States v. Jones*, 2011 WL 1456728 (June 27, 2011), U.S.S.C. Docket No. 10-1259.

.../6

- 6 -

The supervision provided by prior judicial authorization, the criminal trial process, and complaint-driven oversight under police and privacy-related statutes, while critical, are fundamentally insufficient. Let me explain.

The proposed surveillance and access regime will frequently involve complex, highly technical, and sensitive information. Moreover, where prior judicial authorization is required, the relevant surveillance and access applications are necessarily held *in camera* and *ex parte*. Where the resultant surveillance and access activities produce legal charges that lead to a criminal trial, the trials invariably have a narrow focus on the accused. National security-related investigations, which often have a much broader focus, invariably proceed in secrecy, and are rarely subject to public scrutiny. In both contexts, innocent individuals subject to surreptitious invasions of their privacy may never be in a position to learn about, let alone file for or find any redress. In addition, existing complaint regimes are limited as to their reach, powers and remedies. Any in depth public scrutiny of such matters will be the *rare* exception to a general rule of confidentiality and secrecy.

Furthermore, under the Bills, local, provincial, and federal law enforcement agencies will be equally empowered to use these intrusive powers in pursuit of both domestic and international investigations. Without a focused harmonizing and coordinating authority, inconsistent policies and practices are likely to develop among the various jurisdictions. Inevitably, privacy rights and civil liberties will suffer from fragmented and inconsistent protections.

Canadians have a *constitutional* right to be secure from unreasonable search and seizure. The expansive surveillance proposals bring this right into question. And, since the state's authority to intrude on privacy does not come with concomitant responsibilities with respect to accountability, notification and transparency, the net negative effect on human rights is likely to be compounded over time.

To its credit, the government has responded to recent court rulings⁵ by including a provision in Bill C-50 that will require that: (i) a person who has been the target of a warrantless exceptional circumstances interception must be notified of the interception within a specified period; and (ii) the relevant Minister must report publicly on police resort to such warrantless wiretaps.

At the same time, we note that these notice and reporting mechanisms are confined to providing a modest degree of notice, transparency and accountability (restricted as they are to only notifying the *target* of the surveillance, and confined as they are to limited numeric reporting) with respect to a single surveillance power – the power to intercept a private communication. In addition, the reporting practices of provincial and federal Attorneys General with respect to the use of these Part VI wiretap powers have varied considerably (as seen in jurisdictions where the required annual reports have sometimes not appeared until several years have passed).

In this context, we call for the government's public commitment to the enactment of sufficient safeguards to match the array of new and existing powers.

⁵ See *R. v. Six Accused Persons*, [2008] B.C.J. No. 293 (S.C.) and *R. v. Riley*, [2008] O.J. No. 2887 (S.C.J).

- 7 -

Support for this call can be found in recent U.S. and Canadian court decisions. In a unanimous decision of September 6, 2011 requiring the U.S. Department of Justice to publicly disclose information showing the government's use of cell phone location data in criminal prosecutions resulting in a guilty plea or a conviction, the United States Court of Appeals for the District of Columbia determined that:

The disclosure sought by the plaintiffs would inform ... ongoing public policy discussion by shedding light on the scope and effectiveness of cell phone tracking as a law enforcement tool. It would, for example, provide information about the kinds of crimes the government uses cell phone tracking data to investigate. As the plaintiffs note, with respect to wiretapping Congress has balanced privacy interests with law enforcement needs by permitting the government to use that technique for only the more serious offenses ... and the plaintiffs (and others) may decide to argue for similar legislation to govern cell phone tracking. Disclosure would also provide information regarding how often prosecutions against people who have been tracked are successful, thus shedding some light on the efficacy of the technique and whether pursuing it is worthwhile in light of the privacy implications.⁶

And, as indicated above, recent rulings of the Superior Courts of Ontario and British Columbia have determined that notice and reporting safeguards are constitutionally required with respect to intrusive surveillance powers, such as the power Parliament granted peace officers in section 184.4 of the *Criminal Code* (a power to conduct warrantless wiretapping in certain exceptional circumstances). For example, in *R. v. Six Accused Persons*, the B.C. Supreme Court determined that:

Although the Crown submits that in most cases where ... persons whose communications have been intercepted will receive *de facto* notification by way of the prosecution of the underlying offence, that submission fails to recognize that the communications of persons other than the alleged perpetrator may have been intercepted. It also fails to address situations where, for whatever reason, the police may have erred in their assessment of the need to intercept private communications, intercepted more communications than those to which they were lawfully entitled or over a longer period of time, or those that were intercepted under circumstances which did not result in a prosecution.

In any or all of those circumstances, the police would be answerable to no one. Further, the fact that there is no obligation to disclose surreptitious invasions of privacy to those persons whose communications have been intercepted removes an important safeguard to the potential abuse of power that can arise without accountability.

⁶ *American Civil Liberties Union v. United States*, United States Court of Appeals for the District of Columbia Circuit, September 6, 2011, No. 10-5159.

- 8 -

This case is illustrative of some of those concerns ... To this day, many of the persons whose communications were intercepted by the police are unlikely to know of that invasion of their privacy. That circumstance is exacerbated by the police having engaged in the automatic monitoring of all calls to the telephones they had identified as being appropriate for interception. Any discovery by third parties of the police having intercepted their private communications would be fortuitous.

Requirements to notify persons whose private communications have been intercepted of the fact of that interception afford an important constitutional and accountability safeguard to the potential abuse of state power in invading the privacy of its citizens.

The interception of private communications in exigent circumstances is not like situations of hot pursuit, entry into a dwelling place to respond to a 9-1-1 call, or searches incidental to arrest when public safety is engaged. In those circumstances, the person who has been the subject of a search will immediately be aware of both the circumstances and consequences of police action. The invasion of privacy by interception of private communications will, however, be undetectable, unknown and undiscoverable by those targeted unless the state seeks to rely on the results of its intentionally secretive activities in a subsequent prosecution.

I am accordingly satisfied that the failure of ... the [*Criminal Code*] to provide notification of surreptitious interception of private communications to those persons whose communications are intercepted is a serious impediment to the constitutional validity of s. 184.4.

.....
If the intention of Parliament in requiring the provision of [public] reports [enumerating resort to surveillance powers] is to oversee the frequency and circumstances of the interception of private communications by the police, the failure to provide a similar reporting requirement under s. 184.4 of the *Code* removes the potential for that oversight. As with the failure to require notification of those intercepted of the fact of an interception, the lack of any reporting requirement undermines both constitutionality and police accountability.⁷

Bearing all of the above in mind, and in addition to the adjustments we call for to Bills C-51 and C-52, we renew our call for the creation of an independent, arm's-length *Surveillance and Access Review Agency (SARA)*, with a legislative mandate to supervise state access to the highly sensitive personal information associated with digital communications and to report annually to Parliament and the public on the use of the surveillance and access powers.⁸

⁷ *R. v. Six Accused Persons*, [2008] B.C.J. No. 293 (S.C.)

⁸ For more information about the functions and duties we propose for *SARA*, please see our April 21, 2005 letter to the then Minister of Justice and Attorney General of Canada.

.../9

- 9 -

In establishing *SARA*, Parliament would require law enforcement and security agencies who obtain any communication-related data from TSPs to notify all of the individuals whose personal information is involved within one year of the information being obtained unless the individual cannot readily be identified or reasonably located, or notification would prejudice an ongoing investigation. Notification of all readily identifiable individuals would be required within five years of the information being obtained unless, on application to *SARA*, it is determined that the public interest in non-disclosure outweighs the right to notification.

In this context, TSPs should be required to publish annual reports on how many interception and access orders (and requests) they receive a year from which law enforcement and security agencies, in respect of how many individuals; and how many orders (and requests) result in the disclosure of personal information, and in respect of how many individuals.

In renewing the call for the creation of *SARA*, we acknowledge that the preparation and enactment of the necessary legislative framework will take time and that, in the meantime, the government may well decide to proceed with its plan to substantially reshape the state's capacity to conduct surveillance. To the extent that you are not prepared to redraft the Bills to ensure that the new surveillance powers are justified and that the necessary safeguards are in place before the regime comes into force, we strongly urge you to publicly commit to enact a *SARA Act* in tandem with the proposed surveillance and access regime, even as you move to amend the current legislative proposals to provide additional if limited safeguards on it coming into force, as further discussed below.

3) Even with Matching Oversight, the Proposed Powers Require Adjustment

Bill C-51, the *Investigative Powers for the 21st Century Act*, will amend the *Criminal Code*, giving "peace officers" and "public officers" new avenues to obtain access to information generated electronically. As such, a wide range of officers, extending well beyond police, will be empowered to:

- Issue preservation demands on their own say so with respect to a wide array of primarily corporate-held data in the course of investigating any offence, including on behalf of a foreign state, and impose any conditions in the demand that they consider appropriate, including conditions prohibiting the disclosure of its existence or some or all of its contents,
- Apply for new suspicion-based preservation and production orders to preserve and gain access to information about transmission, traffic, communication, tracking, transaction and financial data,
- Apply for new suspicion-based warrants to enable the remote live tracking of vehicles and other things,
- Apply for belief-based warrants to enable the remote live tracking of individuals by tracking the location of cell phones or other things they usually carry or wear, and
- Apply for non-disclosure/secretcy orders with respect to all of the above.

.../10

It is our view that, as a general rule, law enforcement access to data, particularly communications-related data, as well as the new tracking powers, should be subject to prior judicial scrutiny, limited to the investigation of serious crime, generally subject to higher belief rather than suspicion-based thresholds, and come with additional oversight and accountability-related safeguards.

In this context, I note that an August 22, 2011 U.S. District Court decision invites us to raise the question as to the constitutionality of the proposed suspicion-based, as well as belief-based, production order making powers.⁹ In this case, the U.S. government had asked the Court for “orders directing Verizon Wireless, a cell-phone service provider, to disclose recorded information of cell-site-location records for one of its customers pursuant ... to the *Stored Communications Act* or ‘SCA’).” The proposed order sought stored, historical cell-site-location records tied to a period in excess of 113 days. On its face, the *SCA* provides that such an order “may be issued by ... a court of competent jurisdiction ... only if the governmental entity offers specific and articulable facts showing that there are *reasonable grounds to believe* that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.” (Emphasis added.) The Court determined that “the Fourth Amendment to the United States Constitution requires a warrant and a showing of probable cause before the Government may obtain the cell-site-location records requested here.”

As the Court clearly understood, the problem with these kinds of production orders is their implication for the privacy of society at large and, in my view, the concerns expressed by the Court with respect to Americans apply equally with respect to Canadians:

The vast majority of Americans own cell phones. Many Americans have abandoned land line phones entirely, and use cell phones for all telephonic communications. Typically people carry these phones at all times: at work, in the car, during travel, and at home. For many Americans, there is no time in the day when they are more than a few feet away from their cell phones.

Cell phones work by communicating with cell-sites operated by cell-phone service providers. Each cell-site operates at a certain location and covers a certain range of distance. The number of cell-sites that must be placed within a particular area, and thus the distance between cell-sites, is determined by several factors, including population density.

If a user’s cell phone has communicated with a particular cell-site, this strongly suggests that the user has physically been within the particular cell-site’s geographical range. By technical and practical necessity, cell-phone service providers keep historical records of which cell-sites each of their users’ cell phones have communicated.

⁹ *In the matter of an application of the United States of America for an Order authorizing the release of historical cell-site information* No. 10-MC-897, United States District Court, E.D. New York (August 22, 2011).

- 11 -

The implication of these facts is that cellular service providers have records of the geographic location of almost every American at almost every time of day and night. And under current statutes and law enforcement practices, these records can be obtained without a search warrant and its requisite showing of probable cause.

What does this mean for ordinary Americans? That at all times, our physical movements are being monitored and recorded, and once the Government can make a showing of less-than-probable-cause, it may obtain these records of our movements, study the map our lives, and learn the many things we reveal about ourselves through our physical presence.

In the same vein, in the *Maynard* case now pending before the U.S. Supreme Court, the reasoning of the United States Court of Appeals for the District of Columbia provokes questions as to the constitutionality of the proposed suspicion-based, as well as belief-based, *tracking* warrants. As the Appeal Court found in *Maynard*, “prolonged GPS monitoring [of a person’s vehicle travelling on public roads] defeats an expectation of privacy that our society recognizes as reasonable” and must comply with Fourth Amendment standards.

The Court’s holding was echoed as recently as September 21, 2011 in a report issued by the *Liberty and Security Committee* of the U.S. *Constitution Project*. This bi-partisan committee, whose members include two former members of Congress, former FBI director William Sessions, a former U.S. Court of Appeals judge and a former chair of the American Conservative Union, concludes that “when powerful tracking technologies to conduct pervasive surveillance are paired with [a computer’s] analytic capability and a digital database, such monitoring can violate an individual’s reasonable expectation of privacy even in a public place.”

The Committee recommends that, if the U.S. Supreme Court does not adopt the proper approach in the *Maynard* case, Congress should do so by enacting legislation requiring court warrants for any location tracking lasting more than 24 hours.¹⁰

Consistent with these developments, in my view, it is essential that more stringent conditions precedent be enacted in relation to the proposed surveillance and access powers. The use of production orders and tracking warrants should be confined to investigations in respect of the list of serious offences in section 183 of the *Criminal Code*. Before issuing such orders or warrants, a superior court judge ought to be satisfied that:

- There are reasonable and probable grounds to believe that an offence under section 183 of the *Criminal Code* has been or is being committed,
- Other less intrusive investigative methods are likely to prove impracticable,

¹⁰ See the Liberty and Security Committee September 21st, 2011 *Statement on Location Tracking* at <http://www.constitutionproject.org/pdf/LocationTrackingReport.pdf>

- 12 -

- Measures will be taken to safeguard the privacy of the personal information obtained, particularly of non-suspects, and
- The intrusion is otherwise in the best interests of the administration of justice.

As indicated, Bill C-51 also proposes to create a new set of powers that police could invoke to require data managers to locate and hold personal information in documents or databanks. Government has argued that these preservation powers are necessary to support the production order powers discussed above. In our view, any power to issue a preservation demand or order should be confined to the same list of serious offences in section 183 of the *Criminal Code*.

In addition, in order to address the risk to accountability that non-disclosure or secrecy orders entail, we recommend that all those whose personal information is obtained under a surveillance and access regime should be entitled to notification at the appropriate time. And, in accord with our *SARA*-related recommendations, state use of these powers and access to this personal information should be superintended and reviewed by an independent agency.

It is also noteworthy that in introducing sections 487.0195(1) and (2) to the *Criminal Code*, Bill C-51 provides broad immunity from “any criminal or civil liability” to any person who voluntarily preserves data or provides a document to an officer. The person is no longer required to show that he or she acted on reasonable grounds *per* the operation of what is now section 487.014 with section 25 of the *Criminal Code*. The person need only show that his or her cooperation was not “prohibited by law.” In our view, individuals and entities responsible for safeguarding personal information of members of the public must act reasonably before they should be entitled to such immunity. A reasonableness standard provides volunteers with significant protection while helping to rule out the possibility that, for example, malicious or incompetent decision makers will enjoy undeserved immunity.

Accordingly, section 487.0195(2) should be amended to provide that:

A person who preserves data or provides a document in the circumstances described in subsection (1) does not incur any criminal or civil liability for doing so if he or she acted reasonably in the circumstances.

Bill C-50, the *Improving Access to Investigative Tools for Serious Crimes Act*, will amend the *Criminal Code*, first by providing that if a wiretap authorization is granted under Part VI, the judge may at the same time issue one or more Bill C-51-related warrants or orders that relate to the investigation in respect of which the wiretap authorization is given. That is, in obtaining a wiretap warrant, police may also contemporaneously obtain companion production orders and tracking warrants, all from a single judge. Rules respecting secrecy and confidentiality that apply in respect of a wiretap authorization will also apply in respect of a request for a related warrant or order. In addition, the Bill will permit a peace officer or a public officer to install and make use of a number recorder without a warrant in exigent circumstances. The Bill will also extend to one year the maximum period of validity of a warrant for a tracking device and a number recorder if the warrant is issued in respect of a terrorism offence or an offence relating to a criminal organization (the maximum is now 60 days).

.../13

The critical development brought forward in Bill C-50 is that the efficiencies it may purchase in streamlining the conduct of judicially authorized state surveillance and access may come at some cost to the rigour of prior judicial scrutiny. In some cases, a single judge hearing a multitude of inter-related applications may be better informed about the extent of the overarching surveillance employed. At the same time, the demands on judges are likely to grow. In the context of what are necessarily *ex parte* and *in camera* proceedings, there will be an increased risk that a greater degree of intrusive surveillance and access will be granted in cases where it is not warranted. While we do not oppose Bill C-50 *per se*, its enactment will likely intensify the effect of the new surveillance regime. Such intensification increases the need for the adoption of matching safeguards under a *SARA Act*.

4) Surveillance Must Not Undercut the Future of Freedom, Innovation and Privacy

In addition to the controversial plan to provide law enforcement with warrantless access to subscriber information (discussed in section 5 below), the *Electronic Communications Act* sets in motion a fundamental change to the way communication services are regulated. It does so by entrenching the power of security officials to require TSPs to:

- Build in and continuously maintain a wide array of yet to be specified interception capabilities into all their networks, systems and software for the purpose of allowing authorized agencies to intercept, isolate and accurately correlate multiple communications per court orders,
- Notify law enforcement and CSIS officials regarding changes to state provided equipment or systems where those changes are likely to reduce interception capability;
- Assist designated persons who will have warrantless access to TSP facilities, systems, documents and information to test, inspect, and access TSP facilities, services and systems for regulatory purposes,
- Provide prescribed specialized telecommunications support to CSIS and law enforcement agencies,
- Submit lists of TSP personnel to CSIS and/or the RCMP for the purposes of conducting security assessments of employees who may assist in the interception of communications, and
- Comply with prescribed confidentiality and security measures.¹¹

The *Electronic Communications Act* will also establish numerous offences and violations and subject TSPs, their officers, directors, and employees to prosecution and fines for failing to comply with obligations, including those relating to systems requirements.

¹¹ Note that, to date, security officials have been able to impose a similar framework largely outside Parliamentary scrutiny through, for example, the Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications, and Conditions of Licence for New Cellular and PCS Licences issued by the Minister of Industry under the *Radiocommunication Act* (see <http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf09251.html>).

Each additional day in breach of the statute will add to the count of violations and increase the exposure of TSPs, their officers, directors, and employees to fines of up to \$50,000 per offence for an individual and \$250,000 for a corporation. The *Electronic Communications Act* will allow the state to seek a court injunction ordering a TSP to cease operating a transmission apparatus, or to refrain from acquiring, installing or operating new software, if the TSP is contravening or likely to contravene interception requirements.

It is also noteworthy that the *Electronic Communications Act* does not address the financial and commercial implications of these proposals, either to businesses, consumers, or taxpayers. It only authorizes the payment of some monies to compensate TSPs in relation to: (i) compliance with a Ministerial order to provide interception capabilities additional to those prescribed; (ii) the provision of subscriber information; and (iii) the provision of certain specialized telecommunications support. Reports about the cost of related proposals in the U.S. and the U.K. warrant careful consideration in Canada.

In October of 2010, it was reported that, in response to the Obama administration's intention to submit comparable surveillance legislation, American TSPs are "likely to object to increased government intervention in the design or launch of services. Such a change ... could have major repercussions for industry innovation, costs and competitiveness."¹²

In the U.K., a related though more intrusive data retention and "Interception Modernization Program" was being considered until it was abandoned by the British government in late 2009 because of concerns about cost, controversy and feasibility. Prior to this, it was reported that development costs will be high (2 to 13 billion pounds). "The bulk of the costs will be incurred by [TSPs]. The most ignored cost comes in the form of opportunity costs as engineers will be tasked to develop this [surveillance] solution instead of developing their core business, *i.e.* new ways to enhance the networks for advancing consumer and business interests."¹³

None of these immediate financial costs would necessarily translate into privacy issues *per se* if it were not for the fact that the *Electronic Communications Act* risks causing additional marketplace distortions by effectively prohibiting the use and development of any systems or software that might impair a TSP's capacity to facilitate simultaneous multiple intercepts. While the goal of facilitating compliance with court ordered surveillance is valid, there is a significant risk that in implementing this legislation, the authorities will impede the development and use of new communications technologies and services, particularly, for example, privacy enhancing technologies and services such as those that provide for encryption.

In this regard, the *Electronic Communications Act* requires that a TSP must "use the means in its control" to provide an intercepted communication "in the same form as it was before the communication was treated by the service provider" by way of encoding, compression, or encryption. A TSP is not required to make the form of an intercepted communication the same as it was before the communication was treated if it would be required to develop or acquire new

¹² "Officials Push to Bolster Law on Wiretapping", Charlie Savage, New York Times, October 18, 2010.

¹³ London School of Economics, *Briefing on the Interception Modernisation Programme*, June 2009, p. 44-45.

- 15 -

decryption techniques or tools. The legislation appears to allow companies like Research in Motion to continue to provide existing encryption protected communication services. It remains to be seen what the future holds for new companies and new strong encryption techniques and services in the field of communications. For example, there is a risk that the *Electronic Communications Act* will set the stage for rules requiring back-door state access to encryption services.

It is evident that many of the critical details flowing from the *Electronic Communications Act* will be left to policies, procedures, regulations and evolving relationships between TSPs and the state. In passing so many significant public policy decisions on to security-oriented officials, Parliamentarians and the public risk being left out of the decision-making process and Canadians risk seeing TSPs transformed into agents of the state. This represents a significant and needless risk to a free and open society.

We only have to look to recent U.S. history to consider the implications. Many will now be familiar with reports of the secretive and controversial assistance that major telecommunications carriers provided the National Security Agency in the conduct of warrantless eavesdropping on international calls by suspected terrorists after 9/11. As recognized by U.S. courts, such surveillance has the potential to expose “journalistic sources, witnesses, experts, foreign government officials, and victims of human rights abuses located outside the United States” to “violence and retaliation by their own governments, non-state actors, and the U.S. government.”¹⁴

While the *Electronic Communications Act* will be subject to a form of Parliamentary review five years out, in the meantime, if passed, it will substantially alter the design and operation of communication systems, the role and function of TSPs, their ability to be transparent, and the relationship between citizens, TSPs and the state.

A comprehensive and public cost benefit analysis should *precede* rather than follow the making of so many significant public policy decisions. Before imposing the kind of interception capacity regime the *Electronic Communications Act* would impose on TSPs, Parliament should ensure that such a capacity regime will be proportionate and designed to ensure not only appropriate surveillance capacity but also necessary competitiveness and privacy.

It follows that the Parliamentary committee eventually mandated to consider the kinds of proposals in the *Electronic Communications Act* should be adequately resourced to ensure that civil society, as well as industry, has a full opportunity to provide substantial input.

In addition, the *Electronic Communications Act* should be amended to require that all interception-related capacity requirements be *publicly* vetted for their impact on privacy and competitiveness *before* they are imposed (in the future, *SARA* should have a role to play in reporting on the impact of capacity-related requirements). Such requirements should be

¹⁴ *Amnesty Int'l USA et al. v. Clapper et al.*, United States Court of Appeals for the Second Circuit, September 21st, 2011, 09-4112-cv, at pages 8-9 of Circuit Judge Lynch's decision, quoting from *Amnesty Int'l USA v. Clapper*, 638 F.3d 118 (2d Cir. 2011).

.../16

- 16 -

provided for in the form of draft regulations which would only come into force after a vote by Parliament to approve them as a whole.

5) Warrantless Access to Subscriber Information Must Be Withdrawn

In addition to providing the state with substantial control over the design and operation of TSP systems, the *Electronic Communications Act* will also provide law enforcement and CSIS officials with *warrantless* access to subscriber information for the purposes of performing *any* of their duties or functions. Subscriber information includes a named individual's IP address or mobile ID number, or the name and contact information of a subscriber associated with an IP address or mobile ID number.

The *Electronic Communications Act* provides for attenuated *post facto* review of warrantless access to subscriber information. In doing so, it relies on provincial and territorial privacy commissioners to: (i) conduct audits to assess local and provincial police compliance with provisions of the statute empowering the collection and use of subscriber information; and (ii) review police reports generated to the extent that police decide that something has occurred with respect to their own exercise of these access powers that, in their opinion, ought to be brought to the attention of the responsible provincial minister (in Ontario, the attorney general).

Under section 20(6) of the legislation, the Privacy Commissioner of Canada must provide Parliament with an annual report identifying the provincial and territorial privacy commissioners who may receive any such opinion-based reports and the powers that they have to conduct section 20 compliance audits.

Like a number of other provincial and territorial privacy commissioners, I lack the necessary powers. In particular, under Ontario's privacy statutes, I do not have any audit powers. Even those privacy commissioners with sufficient powers are likely to need additional resources in order to adequately perform the legislative duties imposed under section 20 of the *Electronic Communications Act*.

In a letter of March 9, 2011 signed by all the federal, provincial and territorial privacy commissioners, we joined our colleagues in calling on the federal government to commit to working with provincial and territorial governments to ensure that all of our offices have sufficient powers and resources should the *Electronic Communications Act* be enacted. It does not appear that any such commitment has been forthcoming.

Quite apart from the constitutional issues raised by the enactment of a regime of warrantless access, it is noteworthy that in some circumstances, aspects of *post facto* oversight of communications-related surveillance powers have been found by Superior Courts to be constitutionally required (see, for example *R. v. Six Accused Persons*, [2008] B.C.J. No. 293 and *R. v. Riley*, [2008] O.J. No. 2887). In the absence of the necessary provincial and territorial powers and resources, the *Electronic Communications Act's* reliance on provincial and territorial privacy commissioners is untenable. In addition, the audit duties to be imposed on provincial and territorial privacy commissioners under section 20 may raise division of powers problems.

.../17

It remains our view that the *Electronic Communications Act* should be amended to require that provisions setting out TSP obligations concerning “subscriber information” should be deleted and replaced with a court supervised regime.

“Subscriber information” is personal information. To date, all individual customers enjoy the legal right to insist that, subject to narrowly defined exceptions, their subscriber information remains private and confidential. The law currently provides for warrant procedures, expedited tele-warrants, and an organization’s special exercise of discretion to disclose personal information to law enforcement without an individual’s consent, for example, in aid of an Internet-related child pornography investigation, or in comparable exigent-like circumstances. Granting law enforcement and intelligence officials an almost unfettered power to issue their own administrative “warrants” for the purposes of performing *any* of their duties or functions is a substantial departure from the legal and constitutional framework in Canada. Such a departure requires extraordinary justification and a substantial framework for accountability.

Consistent with our earlier comments, law enforcement and security agency access to information linking subscribers to devices (and *vice versa*) should generally be subject to prior judicial scrutiny accompanied by the appropriate checks and balances. Before issuing an order requiring the disclosure of subscriber information, a judge ought to be satisfied that:

- There are reasonable and probable grounds to believe that an offence under section 183 of the *Criminal Code* has been or is being committed,
- Measures will be taken to safeguard the privacy of the personal information obtained, particularly of any non-suspects, and
- The intrusion is otherwise in the best interests of the administration of justice.

In the alternative, if Parliament is determined to allow warrantless access to subscriber information, the legislative safeguards in section 20 of the *Electronic Communications Act* should be strengthened so that they provide a much greater degree of *post facto* oversight. In particular:

- The power to demand warrantless access to subscriber information should be narrowed to only apply in circumstances where access is necessary to the investigation of a specific and defined category of serious crime, for example, sexual offences involving children and minors, or to prevent or eliminate a significant and imminent risk of serious bodily harm.
- The “consistent use” limitation regarding subscriber information collected by law enforcement and security agencies should be strengthened. A use should only be considered as consistent if a reasonable person might reasonably have expected such a use.

- 18 -

- Law enforcement and security agencies should be required to securely destroy information that is provided in response to a subscriber information request one year after the individual has been notified of its collection, or once retention of the information is no longer necessary for the purpose for which the information was obtained, or for a use consistent with that purpose, whichever is later.
- The requirement that law enforcement and security agencies must report to attorneys general and privacy commissioners should be strengthened. Agencies should be expressly required to report any collection, use or retention practices that do not appear to be necessary and proportionate in relation to the duty or function for which they were originally obtained.
- In reporting to Parliament on the adequacy of audit and investigation powers available to provincial and territorial privacy commissioners, the Privacy Commissioner should also report on whether those commissioners consider themselves to have adequate resources to conduct the necessary audits and reviews.
- If, after consulting with a provincial or territorial commissioner, the Privacy Commissioner reports that her colleague does not have substantially similar powers, the subscriber information powers available to police services within that jurisdiction should *automatically* lapse until the Privacy Commissioner reports back that the provincial or territorial commissioner has been provided with those powers.

To the extent that Parliament chooses to rely on provincial and territorial privacy commissioners to perform *post facto* review of warrantless access to subscriber information, it follows that the federal government must commit to working with provincial and territorial governments to ensure that all of the relevant privacy commissioners have sufficient powers and resources. In this regard, please note that I have written two letters to Ontario's Attorney General, asking that the Ontario government play its part in these important law reform and oversight-related issues. Copies of those letters are attached.

Conclusion

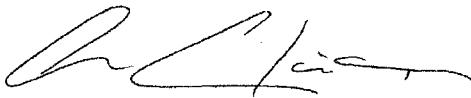
The surveillance regime being put forward is aimed at capturing the full range of content, communication and traffic data associated with digital communications. As communication services continue to evolve, the legislation will empower the state to develop, update and enforce regulations directly aimed at shaping the technological capacities of telecommunication services so as to ensure that Web 2.0, 3.0 etc. communications can be readily intercepted, isolated and accurately correlated. In this context, it is reasonable to foresee that it will be much easier for the state to subject more individuals, including innocent individuals, to unwanted surveillance and scrutiny.

.../19

- 19 -

This debate is not about maintaining the state's surveillance capabilities, but trying to determine the proper balance in the evolving information age. In the face of so many significant changes, with so much at stake, and with so much left to regulation and implementation by policy, we are concerned that the public, Parliament and industry will be hard pressed to keep abreast of the technological challenges, the financial costs, and the invasiveness of an *expanding surveillance regime*. It is essential that Parliament and the public be well informed on technological, legal, regulatory and financial issues. The implications for privacy and other human rights must also be fully addressed, by providing for the necessary transparency, accountability and oversight. No less than the future of privacy – the future of freedom, is at stake.

Yours sincerely,



Ann Cavoukian, Ph.D.
Commissioner

Enclosures (2)

c: The Honourable John Gerretsen, Attorney General of Ontario
William Baker, Deputy Minister, Public Safety Canada
Myles Kirvan, Deputy Minister of Justice & Deputy Attorney General of Canada
Murray Segal, Deputy Attorney General of Ontario



Information and Privacy
Commissioner/Ontario
Commissaire à l'information
et à la protection de la vie privée/Ontario

VIA EMAIL AND COURIER

October 24, 2011

The Honourable John Gerretsen
Attorney General of Ontario
Ministry of the Attorney General
McMurtry-Scott Building
720 Bay Street, 11th Floor
Toronto, ON M7A 2S9

Dear Minister Gerretsen:

I am writing to congratulate you on your appointment as the Attorney General of Ontario. While I have enjoyed a good working relationship with you in your previous Ministry, I look forward to working with you in your new capacity. In this regard, I think we may both benefit from an opportunity to meet briefly in person, perhaps early in the new year. If you are interested, my office will be in contact with yours to confirm a date and time.

In addition, I attach a copy of my September 23rd, 2011 letter to Minister Bentley, with whom my office also enjoyed a productive relationship, regarding section 20 of Bill C-52, the *Investigating and Preventing Criminal Electronic Communications Act (ECA)*. While this and two other related bills died on the Order Paper at the end of Parliament, I understand that the federal government intends to re-introduce all three shortly, in essentially the same format.

Over the last few weeks, public dismay about the likely re-introduction of Bills C-50, C-51, and C-52 has been growing. Many of the grave concerns that I and other privacy commissioners have had about these proposals were reflected in the October 22nd, 2011 article in the National Post, *Laws for 21st century: A guide to Canada's proposed cyber investigation bills* (copy attached).

Read together, their enactment would substantially diminish the privacy rights of Canadians. They would do so by enhancing the capacity of the state to conduct surveillance, as well as access private information, while reducing the frequency and vigour of judicial scrutiny, thus making it easier for the state to subject more individuals to expanded surveillance and scrutiny.

My concerns about these legislative proposals can be summarized as follows:

- The proposed surveillance powers come at the expense of the necessary privacy protective constitutional balance. In order to maintain that crucial balance, the federal government must be persuaded to acknowledge the sensitivity of traffic data, stored data, and tracking data and to re-draft the bills accordingly.



2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

.../2
Tel: 416-326-3333
1-800-387-0073
Fax/Télééc: 416-325-9195
TTY: 416-325-7539
www.ipc.on.ca

000417

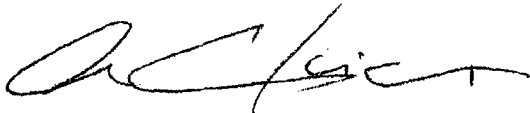
- 2 -

- Intrusive proposals require matching legislative safeguards. The courts, affected individuals, future Parliaments, and the public must be well informed about the scope, effectiveness, and deleterious effects of intrusive powers. If the federal government pushes ahead with expansive new surveillance powers, I hope you will join me in urging the federal government to publically commit to enacting the necessary oversight legislation, in tandem.
- Even with matching oversight, the proposed surveillance and access powers require more stringent conditions precedent.
- Entrenching a mandatory surveillance capacity regime on the public and its telecommunications service providers (TSP) must not go forward without adequate safeguards to protect the future of privacy and freedom; a comprehensive cost-benefit analysis, made publicly available, should precede rather than follow the making of so many significant public policy decisions. Public Parliamentary hearings should also be scheduled to ensure that civil society, as well as industry, have a full opportunity to provide substantial input on all of the bills, including the *ECA*.
- The proposal for warrantless access to subscriber information is untenable and should be totally withdrawn. It remains our view that the *ECA* should be amended to require that the provisions setting out TSP obligations concerning "subscriber information" be deleted and replaced with a court supervised regime.

While I continue to have the specific concerns about the focused legal and fiscal issues outlined in my September 23rd letter, I believe it is increasingly important for you to be aware of the *overarching* surveillance and access proposal and the serious implications it has for the privacy rights of the residents of Ontario as a whole.

Once again, congratulations on your appointment. I wish you every success in the important work ahead.

Sincerely yours,



Ann Cavoukian, Ph.D.
Commissioner

Enclosure



Information and Privacy
Commissioner of Ontario
Commissaire à l'information
et à la protection de la vie privée de l'Ontario

September 23, 2011

VIA EMAIL AND LETTER MAIL

The Honourable Chris Bentley
Attorney General of Ontario
Ministry of the Attorney General
McMurtry-Scott Building
720 Bay Street, 11th Floor
Toronto, ON
M7A 2S9

Dear Minister Bentley:

I am writing you in relation to a single aspect of the federal government's anticipated package of surveillance-related legislation. My concerns focus on the legal and fiscal factors likely to undermine my capacity to fulfil the role the federal government purports to assign to my office under section 20 of Bill C-52, the *Investigating and Preventing Criminal Electronic Communications Act* (hereafter referred to as the *Electronic Communications Act* or *ECA*). While this bill died on the Order Paper at the end of the last Parliament, I understand that the federal government may re-introduce it in essentially the same form shortly.

In addition to providing the state with substantial control over the design and operation of "telecommunication service providers" (TSP) systems, the *Electronic Communications Act* would provide law enforcement and CSIS officials with warrantless access to *subscriber information* for the purposes of performing any of their duties or functions. *Subscriber information* includes a named individual's IP address or mobile ID number or the name and contact information of a subscriber associated with an IP address or mobile ID number.

Access to TSP-held *subscriber information* will empower police to link specific communication devices with particular individuals, as well as to monitor a wide range of their communications and activities in cyberspace. Since this power would be available for the purposes of performing *any* police duties or functions, the potential benefits and risks will be comparably wide ranging.

Section 20 of the *ECA* provides for attenuated *post facto* review of warrantless access to subscriber information. In doing so, it relies on provincial and territorial privacy commissioners and ombudsmen ("public officers" or "privacy officers") to: (i) conduct audits to assess local and provincial police compliance with provisions of the Bill that broadly empower the collection and use of subscriber information; and (ii) review police reports generated after police determine that something has occurred with respect to their own exercise of these access powers that, in their opinion, ought to be brought to the attention of the responsible provincial minister (in Ontario, the Attorney General).

.../2



Legal Services Department
2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

Services juridiques
2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel: 416-326-3333
1-800-387-0073
Fax/Télé: 416-325-9186
TTY: 416-325-7539
www.ipc.on.ca

000419

- 2 -

Under section 20(6) of the *ECA*, the Privacy Commissioner of Canada must provide Parliament with an annual report identifying the provincial privacy officers who may receive any such opinion-based reports and the powers that they have to conduct section 20 compliance audits.

In my case, I lack the powers necessary to fulfill the proposed duties. In fact, under our home statutes, I do not have any audit powers. This may be the case for other provincial and territorial officers. This concern was reflected in a letter of March 9, 2011 signed by all the federal, provincial and territorial privacy officers. In that letter, we joined our colleagues in calling on the federal government to commit to working with provincial and territorial governments to ensure that all of our offices have sufficient powers and resources should the *Electronic Communications Act* be enacted. It does not appear that any such commitment has been forthcoming.

As I am sure you will agree, under these circumstances, the federal government's approach to oversight is clearly untenable. Quite apart from the constitutional issues raised by the enactment of a regime of warrantless access, it is noteworthy that in some circumstances, aspects of *post facto* oversight of communications-related surveillance powers have been found to be constitutionally required (see, for example *R. v. Six Accused Persons*, [2008] B.C.J. No. 293] and *R. v. Riley*, [2008] O.J. No. 2887). In addition, the audit duties to be imposed on my office under section 20 may raise division of powers problems.

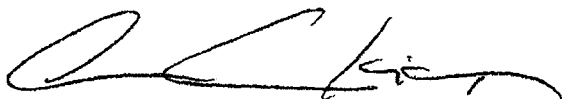
Finally, I note that I would lack the necessary fiscal and human resources required to adequately perform the legislative duties imposed under the *Electronic Communications Act*.

While it continues to be our view that the *Electronic Communications Act* should be amended to ensure that police access to *subscriber information* is subject to a system of prior judicial authorization, it appears likely that the federal government will move ahead with a system of warrantless access and attenuated *post facto* review.

In this context, I wanted to alert you to the federal government's apparent failure to account for these significant problems and to urge you to raise these matters with your federal counterparts. Should they insist on proceeding in this direction, you may be faced with having to address uninvited legislative, fiscal, and constitutional issues.

Please do not hesitate to contact me if you wish to discuss these matters further.

Sincerely yours,



Ann Cavoukian, Ph.D.
Commissioner

cc: Murray Segal, Deputy Minister

Brock, Darlene

From: Travers, Evan
Sent: Tuesday, April 12, 2011 5:26 PM
To: Brock, Darlene
Cc: Banerjee, Ritu; Davies, John; Galadza, Larisa; Coburn, Stacey; Nixon, Jennifer
Subject: NSPD input - paper on OPC

Importance: High

Attachments: OPC - presentation to SECU.DOC; PS-SP-#406086-v2-Memo_to_DM_-_Privacy_Commissioner_Visit_April_14__2011.DOC

Darlene,

Please find below NSPD's response to your request for additional information regarding the note to the DM on the Privacy Commissioner's scheduled 14 April 2011 presentation to the Executive Committee. This response has been approved by John Davies, DG, NSPD.

Please don't hesitate to contact me if you have any questions.

Best regards,
Evan.

1. "A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century"

We suggest the following be appended to the paragraph on the "Matter of Trust" paper:

"Along with other stakeholders, Public Safety participated in a half-day session on the document during its development. The use of the word "integrating" in the title is in direct recognition that security and privacy should both be pursued to the greatest extent possible; a comment in the consultation process was that terms such as balance connote trade-offs, and most around the table agreed that trade-offs are not always necessary. The paper discusses at some length the social value that is derived from strong protections for privacy, but does not offer a similar description of the social value of security - an omission that Public Safety had pointed out to the OPC, but that was not accepted by that Office. As committed to in the Air India Inquiry Action Plan, Public Safety is presently developing legislation to clarify authorities for information for national security purposes."

2. Passenger Protect Program

We suggest the following be appended to the paragraph on the Passenger Protect Program:

"Public Safety Canada is currently developing Privacy Impact Assessments for both the Office of Reconsideration and the Specified Persons Advisory Group under the Passenger Protect Program to ensure compliance with the *Privacy Act* and relevant Treasury Board policies. To that end, Public Safety is developing Personal Information Banks and Memoranda of Understanding to govern information sharing under the Passenger Protect Program."

3. National Security Review

We suggest adding the below as a new bullet, immediately following the paragraph on the Passenger Protect Program:

"In May 2009, Ms. Stoddart appeared before the Standing Committee on Public Safety and National Security during its review of the Iacobucci (Almalki, Elmaati and Nureddin) and O'Connor (Arar) Inquiries. Among other things, Ms. Stoddart encouraged an integrated approach to national security oversight: "[I]f I can leave you with one overarching message, it

000421

would be this - in an era of networked intelligence and surveillance, Canada needs a networked approach to oversight and review. Proper oversight and accountability for national security provide a vital check for Canadians' privacy rights." [The text of Ms. Stoddart's presentation to the Committee is attached ("OPC – presentation to SECU.doc").] As committed to in the Air India Inquiry Action Plan, Public Safety is presently undertaking policy work to enable the review of national security activities involving multiple departments and agencies, and to create an internal mechanism to ensure accountability and compliance with the laws and policies governing national security information sharing."

4. Relationship with the Privacy Commissioner

We suggest adding the below as a new paragraph, immediately prior to the paragraph on the Privacy Impact Assessment Framework:

"The Privacy Commissioner is and will continue to be an important interlocutor in the development of a number of Public Safety policy initiatives. As such, this presentation to the Executive Committee will be an opportunity to continue to build a productive relationship with her Office, while recognising our limited ability to discuss details of policy development that are protected by Cabinet confidence. It would be useful to seek the Privacy Commissioner's input, even if in a generic sense, early on in the process so that her input can meaningfully inform our analysis of options."

--

Evan Travers

Senior Policy Analyst | Analyste principal des politiques
National Security Policy | Politiques sur la sécurité nationale

Public Safety Canada | Sécurité publique Canada
269 Laurier Avenue West | 269, avenue Laurier ouest
Ottawa, Canada K1A 0P8

Tel. | tél.: 613.949.3184
Evan.Travers@ps-sp.gc.ca

Government of Canada | Gouvernement du Canada



OPC - presentation PS-SP-#406086-v2-
to SECU.DOC... Memo_to_DM_-_...



Public Safety Sécurité publique
Canada Canada

Ottawa, Canada
K1A 0P8

Seen by the DM
Vu par le SM

DEPUTY MINISTER'S OFFICE
PUBLIC SAFETY CANADA

2011 APR 13 P 2:00

AVR 14 2011
APR

UNCLASSIFIED

DATE: APR 13 2011

File No.: CR-8221-132 / 379099
RDIMS No.: 406086

MEMORANDUM FOR THE DEPUTY MINISTER

PRIVACY COMMISSIONER JENNIFER STODDART'S APPEARANCE
PUBLIC SAFETY EXECUTIVE COMMITTEE

(For information)

ISSUE

To inform you of the privacy issues implicating Public Safety in advance of Commissioner Stoddart's appearance at the Executive Committee meeting of April 14, 2011.

BACKGROUND

The Office of the Privacy Commissioner (OPC) has identified its four top strategic priorities as being Information Technology, National Security, Identity Integrity and Protection and Genetic Information. As a result of these priorities, it is anticipated that Commissioner Stoddart will discuss primarily the initiatives and programs of Public Safety that involve national security, and the role of privacy in security initiatives. An outline of the OPC's recent appearances and documents by the OPC concerning public safety and national security is as follows:

- The Privacy Commissioner has expressed concern with aspects of the subscriber information provisions of proposed lawful access legislation. The concerns relate to her perception that the subscriber information component is too broad and allows unrestricted access to such information, and does not contain sufficient review/oversight mechanisms. The Commissioner has also expressed concern with previous

.../2

UNCLASSIFIED

- 2 -

legislative proposals allowing authorities to request subscriber information without first accessing a judicially authorized warrant. These concerns were raised in her 2009-2010 annual report to Parliament and again highlighted to you in a March 9, 2011, letter signed by Commissioner Stoddart and all provincial and territorial privacy Commissioners. In your April 12th response, you highlighted how the Government appreciates the need to strike the right balance between the privacy of Canadians and its investigative and policing requirements. You indicated that your officials would continue to explore options to further protect Canadians' privacy rights in any future legislative proposals. The Privacy Commissioner, as well as many of her provincial and territorial counterparts, participated in past lawful access consultations and their concerns have informed the development of the privacy safeguards in the various legislative proposals over the years. We anticipate that this dialogue will continue.

- In February 2011, the Assistant Privacy Commissioner, Mme. Chantal Bernier, addressed the Centre for National Security organized by the Conference Board of Canada concerning the issue of cyber security as it relates privacy. With respect to the Cyber Security Strategy, she indicated the OPC looks forward to supporting the third pillar of the Strategy – Helping Canadians be Secure Online - through their ongoing commitment to public education and outreach.
- In November 2010, the Office of the Privacy Commissioner released a reference document entitled “A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century”. The aim of the document was to present the analytical framework and basic steps used by the Office of the Privacy Commissioner when examining new public safety measures and to aid in integrating privacy concerns within security initiatives. Along with other stakeholders, Public Safety participated in a half-day session on the document during its development. The use of the word “integrating” in the title is in direct recognition that security and privacy should both be pursued to the greatest extent possible; a comment in the consultation process was that terms such as balance connote trade-offs, and most around the table agreed that trade-offs are not always necessary. The paper discusses at some length the social value that is derived from strong protections for privacy, but does not offer a similar description of the social value of security - an omission that Public Safety had pointed out to the OPC, but that was not accepted by that Office. As committed to in the Air India Inquiry Action Plan, Public Safety is presently developing legislation to clarify authorities for information for national security purposes
- In November 2009, the Office of the Privacy Commissioner published a report on the Audit of the Passenger Protect Program at Transport Canada. The Audit report noted that Transport Canada had made changes to comply with recommendations dealing with information provided to the DM and with the department's oversight role of

.../3

000424

UNCLASSIFIED

- 3 -

airlines under the program; and that commitments were also made to undertake activities to improve its practices for the enhancement and protection of Canadians' sensitive personnel information; and review and adjust its existing Certification and Accreditation processes based on best practices and guidelines. The OPC noted that they would conduct a follow-up to this audit exercise in two years to verify progress made in implementing responses to their recommendations. Now that Public Safety has taken over part of this program, the Commissioner may make mention of some of the concerns she had as a result of that audit and what, if anything, the Department may be doing to follow-up on the recommendations. Public Safety Canada is currently developing Privacy Impact Assessments for both the Office of Reconsideration and the Specified Persons Advisory Group under the Passenger Protect Program to ensure compliance with the Privacy Act and relevant Treasury Board policies. To that end, Public Safety is developing Personal Information Banks and Memoranda of Understanding to govern information sharing under the Passenger Protect Program.

- In May 2009, Ms. Stoddart appeared before the Standing Committee on Public Safety and National Security during its review of the Iacobucci (Almalki, Elmaati and Nureddin) and O'Connor (Arar) Inquiries. Among other things, Ms. Stoddart encouraged an integrated approach to national security oversight: "[I]f I can leave you with one overarching message, it would be this - in an era of networked intelligence and surveillance, Canada needs a networked approach to oversight and review. Proper oversight and accountability for national security provide a vital check for Canadians' privacy rights." (The text of Ms. Stoddart's presentation to the Committee can be found in the attached "Evidence" (Tab 1) from the May 7, 2009, meeting of the Standing Committee on Public Safety and National Security, starting at page 3). As committed to in the Air India Inquiry Action Plan, Public Safety is presently undertaking policy work to enable the review of national security activities involving multiple departments and agencies, and to create an internal mechanism to ensure accountability and compliance with the laws and policies governing national security information sharing.

Regarding departmental privacy management, the Privacy Commissioner may point out that Public Safety is not compliant with many Privacy Act and Treasury Board requirements, e.g., for the registration of Personal Information Banks and updating departmental policies following TBS' policy suite renewal. Public Safety has implemented a Privacy Impact Assessment Framework (PIAF) in 2011, and expects to have breach notification guidelines completed in this fiscal year.


.../4

UNCLASSIFIED

- 4 -

The Privacy Commissioner is and will continue to be an important interlocutor in the development of a number of Public Safety policy initiatives. As such, this presentation to the Executive Committee will be an opportunity to continue to build a productive relationship with her Office.

Should you require additional information, please do not hesitate to contact me at 613-949-6435, or Mr. Randall Koops, Director General, Cabinet & Parliamentary Affairs and Executive Services, at 613-949-0477.

 131 April 111

Paul MacKinnon

Attachment (1)

Prepared by: Jennifer Nixon

**Special Extended Executive Committee Meeting
Privacy Commissioner Jennifer Stoddart (and Chris Prince)**

April 14, 2011 from 9:30 to 11:30 a.m.

Executive Boardroom

List of Participants

DMO

William V. Baker
Graham Flack
Josée Dussault
Gabrielle Duschner
Lucie Baulne

COM

Stephanie Durand
Jamie Tomlinson
Andrew Swift

LPB

Richard Wex
Stephen Bolton
Lyndon Murdock

SPB

Paul MacKinnon
Darlene Brock
Jennifer Nixon

EMNS

Lynda Clairmont
Serge Beaudoin for Daniel Lavoie
Jamie Deacon
Gary Donovan
John Davies
Robert Dick

CSPB

Shawn Tupper
Daniel Sansfaçon
Cliff Yumansky

CMB

Rosanna Di Paola
René Bolduc

LS

Caroline Fobes
Sophie Beecher
Ian Bradley

Audit

Rosemary Stephenson
Yolande Andrews
René-Pierre Tremblay

000427



Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada



Office of the Privacy Commissioner of Canada

Home > About Us > Biography of Jennifer Stoddart - Privacy Commissioner of Canada

About Us

- Mandate and Mission
- Organizational Structure
- Commissioner's Message
- External Advisory Committee
- Internal Audit Committee
- Provincial and Territorial Privacy Commissioners and Ombuds Offices
- Access to Information and Privacy
- Privacy Commissioners (1977 to Date)

Biographies



Jennifer Stoddart
Commissioner



Chantal Bernier
Assistant Commissioner
(Privacy Act)

Biography of Jennifer Stoddart - Privacy Commissioner of Canada

Since taking on the role of Privacy Commissioner of Canada in December of 2003 and guiding the Office's institutional renewal after a challenging period in its history, Jennifer Stoddart and the Office of the Privacy Commissioner of Canada have become leaders both nationally and internationally in the privacy sphere.



Ms. Stoddart has overseen a number of important investigations and audits of personal information handling practices in the public and private sectors. She was the first data protection authority to conduct a comprehensive investigation of the privacy policies and practices of the popular social networking site, Facebook. She also investigated a massive data breach at U.S. retail giant TJX, which owns Winners and HomeSense stores in Canada, and, more recently, found that Google Inc. contravened Canadian privacy law when it collected personal information from unsecured wireless networks for Google StreetView.

Ms. Stoddart also led a number of important investigations on the public sector front, and has conducted audits of, for example, the government's personal information disposal practices, its use of wireless technology, the Passenger Protect Program, Passport Canada, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), and the RCMP's Exempt Databanks.

She has led efforts to help public and private sector organizations better understand their obligations under federal privacy law and, particularly, under the *Personal Information and Electronic Documents Act (PIPEDA)* in the first years after the legislation came into force. She recently established a presence in the Toronto region, in order to conduct more on-the-ground outreach and investigation work, and to help mitigate privacy problems before they occur.

Throughout her mandate, she has advocated the need to ensure that both PIPEDA and the *Privacy Act* continue to provide the strongest possible protections for Canadians in an era of constantly evolving risks to privacy.

*Pruned
Chris Stone
Stoddart's
Policy
Analysis*

Biography of Jennifer Stoddart

She has also worked to raise awareness among Canadians of their privacy rights through enhanced communications, outreach and research activities. Ms Stoddart is working to promote online privacy for young people through the Office's website for young people, www.youthprivacy.ca, a blog, contests for high school students, teaching modules and, as the *Globe and Mail* newspaper noted, she "must be the only regulator that has posted a children's video about privacy rights on YouTube."

Given Canada's international trade patterns, Ms. Stoddart has become involved in global privacy issues through her work with international organizations such as the Organization for Economic Co-operation and Development (OECD) and Asia-Pacific Economic Cooperation (APEC), which are examining ways to protect and enhance privacy rights on a global scale. Earlier this year, Ms. Stoddart led an unprecedented collaboration involving 10 data protection authorities who issued a joint letter reminding online companies, such as Google, of their responsibility to respect privacy laws in countries where they launch their products or services. In 2007, she hosted the 29th International Conference of Data Protection and Privacy Commissioners.

The work of the Office of the Privacy Commissioner is guided by four emerging issues that Ms. Stoddart and her team expect will have powerful impacts on privacy in the years ahead. They are: information technology; genetic information; national security; and the integrity of personal identity.

Ms. Stoddart was selected as the 2010 recipient of the International Association of Privacy Professionals' Privacy Vanguard Award for her role in establishing Canada as a leading regulator on privacy issues. She also received the Ontario Bar Association's 2010 Karen Spector Memorial Award for Excellence in Privacy Law, which honours outstanding achievements in the area of privacy law. In 2009, she was awarded the Université du Québec à Montréal's Prix Reconnaissance for her work protecting the privacy rights of Canadians.

Ms. Stoddart has also led a process to strengthen the management and financial framework of the Office of the Privacy Commissioner of Canada. She has strived to continually improved service delivery to Canadians through focus and innovation. Ms. Stoddart has also served on the steering committee of the Group of Heads of Federal Agencies, a network comprising the chief executive officers of more than 100 federal agencies, boards, commissions, tribunals and Crown corporations.

Ms. Stoddart was previously President of the Commission d'accès à l'information du Québec, an organization responsible for both access to information and the protection of personal information. While in this position, she published a report, *The Choice of Transparency*, which led to important changes to Québec's access to information and data protection legislation mandating that government departments and agencies make more information available online.

She has held several senior positions in public administration for the Governments of Québec and Canada since being called to the Québec Bar in 1981.

Ms. Stoddart holds a Bachelor of Civil Law degree from McGill University, as well as a Master of Arts degree in history from the University of Québec at Montréal and a Bachelor of Arts degree from the University of Toronto's Trinity College.

Date Modified: 2010-11-23



House of Commons
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 020 • 2nd SESSION • 40th PARLIAMENT

EVIDENCE

Thursday, May 7, 2009

—
Chair

Mr. Garry Breitkreuz

Also available on the Parliament of Canada Web Site at the following address:
<http://www.parl.gc.ca>

Standing Committee on Public Safety and National Security

Thursday, May 7, 2009

• (0905)

[English]

The Chair (Mr. Garry Breitkreuz (Yorkton—Melville, CPC)): I call this meeting to order.

This is the Standing Committee on Public Safety and National Security, meeting number 20. We are continuing our review of the Iacobucci and O'Connor inquiry reports.

We would like to welcome our witnesses this morning. We have the Office of the Privacy Commissioner, represented by Ms. Jennifer Stoddart, the Privacy Commissioner. She will introduce the people she has with her. As an individual we have Mr. Paul Cavalluzzo.

I understand you have agreed that Mr. Cavalluzzo will go first.

We usually allow approximately 10 minutes for an opening statement. After you've made your opening statement, we'll go to questions and comments.

Without any further ado, we'll go ahead.

Mr. Paul Cavalluzzo (Counsel, As an Individual): Thank you.

Mr. Chair and honourable members, thank you for giving me the opportunity of discussing with you the Arar report, which was presented by Justice O'Connor in September 2006, and part two was delivered in December 2006.

In that regard I acted as his commission counsel in the Arar inquiry, which was conducted over a period of two and a half years. In the limited time I have today in my presentation, I want to focus on the recommendations that were made by Justice O'Connor in parts one and two.

Now I'll give a little background.

As you know, Maher Arar is a Canadian citizen who was stopped at the Kennedy Airport in New York City in September 2002, where he was flying through on his way back to Montreal. He was detained by American officials for 12 days and was subsequently removed to Syria, which is the country of his birth. He was interrogated, tortured, and held in inhumane conditions in Syria for close to one year. On October 5, 2003, he was released and returned to Canada.

To this time, he has never been charged with any offence by Canadians, Americans, or the Syrians. In January 2004 the federal government called a public inquiry because of the political pressure that had been building up in respect of the role of Canadian officials regarding the treatment of Mr. Arar in the United States and Syria.

The public inquiry had two parts. Part one was the factual inquiry, wherein Justice O'Connor looked at what happened and reported on the role of Canadian officials in respect of Mr. Arar's treatment. Part two was the policy review, wherein he was called upon to recommend an independent arm's-length review mechanism for the RCMP in respect of its national security activities.

Now, as far as part one is concerned, the what, why, where, and how, just focusing on the main conclusions, an important part of part one was the information sharing that was conducted by Canadian authorities and in particular by the RCMP. After reviewing all of the evidence, Commissioner O'Connor concluded that the RCMP provided American authorities with information that was inaccurate, unreliable, misleading, and that certainly viewed Mr. Arar in a very negative sense. You must contemplate the context of this. This is a year after 9/11, where the American authorities obviously—as was put by one witness—had a great deal of adrenalin as far as alleged terrorists were concerned.

It was also found that the front-line investigators gave the American authorities, the FBI, information on Mr. Arar that was misleading while he was detained in the United States and while the Americans were interrogating him.

Now, as far as his stay in the United States is concerned, there was no evidence that Canadian officials played any role in the decision of the American authorities to detain Mr. Arar. However, the evidence was clear that American authorities relied upon misleading information that was given to them by the RCMP and that no doubt played a role in his detention by the Americans.

As I said before, after about 12 days they removed Mr. Arar to Syria. Even though they had the option of sending him 200 miles to the border outside of Montreal, they preferred to send him 3,000 miles to Syria because of their view that they didn't want Mr. Arar walking on the streets of Canada.

In Syria, as I said before, it was found that Mr. Arar was tortured and was kept in inhumane conditions for close to a year, and unfortunately, even though Canadian officials, consular officials, had access to Mr. Arar on eight occasions during that time, it was not recognized that he was being tortured at that time because of the manner in which the interviews occurred. Syrian officials were present during the interviews, and unfortunately because of lack of training they did not recognize that he was being tortured.

● (0910)

Upon his return to Canada in October 2003, unfortunately, a lot of information was put out about Mr. Arar that was misleading, that violated national security principles because it was confidential information, and it was made to look as if Mr. Arar was somewhat dangerous and somewhat of a terrorist. Unfortunately, that leaked information has never been reviewed in terms of a criminal prosecution. To this day nothing has happened.

As far as the recommendations of part one are concerned, Justice O'Connor made 23 recommendations. I'll focus on the most important ones.

The first one is on information sharing. Obviously Canada must continue to share information with our foreign partners, but he said that surely we have to screen such information for relevance, reliability, accuracy, and to ensure it complies with our privacy laws.

He also said the RCMP individuals or investigators who are involved in national security must be better trained. They might be great police officers, but that does not mean they're competent to conduct a national security investigation.

He also stated that the RCMP should never provide information to a country with a poor human rights record if the information will cause or contribute in any way to the torture or inhumane treatment of a Canadian held abroad. In other words, Canadians should not be complicit in torture.

The other point he makes in terms of torture is that if we are going to accept information from a country with a poor human rights record, we have to look at the political and the human rights implications of that; and if we are going to accept such information, we had better ensure and assess its reliability, because by definition, such information is usually very unreliable.

Moving to part two of the mandate of the Arar inquiry, which was to make policy recommendations concerning a review mechanism for the RCMP, Justice O'Connor concluded that the existing mechanism for review of the RCMP activities is totally inadequate, for a number of reasons.

Over time, the amount of information sharing the RCMP does has increased immensely. The RCMP now has increased police powers, particularly in the area of national security. A number of practices, such as integrated policing along with other partners, require a more effective review mechanism.

He said that because of the secret nature of national security activities or investigations, it's difficult to monitor that by a complaints-based approach, because people, Canadian citizens, really don't know, for the most part, whether these activities are violating policies and the law and so on.

As a result of that, he recommended that the new review mechanism have the authority to initiate a review of RCMP activities in the national security area on its own. This would be very similar to the power that currently exists with respect to the security intelligence review committee with respect to CSIS operations.

Once again, this kind of power is necessary because these national security investigations are beyond judicial scrutiny, for the most part.

The other important enhancement in terms of a review mechanism that he recommended was that the new review body should be given broad investigatory powers, similar to the powers of a public inquiry. He reviewed the interrelationship between the present CPC and the RCMP and found that it was ineffective because of the limited access to RCMP information the CPC had.

He recommends that this new body have the authority to determine what information it needs to effectively fulfill its mandate. This would involve the power to subpoena, the power to compel testimony, and so on.

● (0915)

The new body, which he called the Independent Complaints and National Security Review Agency for the RCMP—ICRA is the acronym, I guess—would have jurisdiction to review all of the RCMP's activities, not only its national security activities. He said that it's a judgment call, but it's better to have one body reviewing all of the activities of the RCMP, because we need a body that is expert in police work and law enforcement, and so on, and there may be jurisdictional problems if you created separate bodies to review its national security activities and its other activities.

Because of the highly integrated nature of most national security investigations—and the Arar inquiry was a good example of that; we had to review the activity of the RCMP, of CSIS, of the CBSA and so on—he said that other agencies that are involved in national security should be subject to review as well, such as the CBSA, DFAIT, and so on.

Finally—I see my time is running out—he recommended the creation of an overall committee, an independent committee that would be composed of the chair of the new RCMP body, SIRC, the CSIS body, the CSE commissioner, and an independent person, which would review all of the national security review that is done by these bodies, as well as being the place where a citizen would go to file a complaint. Any national security complaint would be filed with this new committee, which would determine which of the three bodies should be involved in its review and also make recommendations concerning national security review policy in the future to the government.

I could go on, but I think it's better to leave more matters for questions.

In conclusion, I would suggest that if we do ever get this kind of effective mechanism for a review of national security activities, there will no longer be a need for these expensive public inquiries and ad hoc inquiries that we have had over the last five years. It's going to be a restructured body, not a completely new bureaucracy, and in our view it'll be effective, efficient, and most importantly, will respect our human rights.

Thank you.

● (0920)

The Chair: Good, thank you very much.

We'll now turn it over to Ms. Stoddart. You can introduce your colleagues and make your opening statement. Go ahead.

May 7, 2009

SECU-20

3

Ms. Jennifer Stoddart (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): Thank you very much, Mr. Chairman, honourable members.

I'm here as the Privacy Commissioner of Canada, and the relevance to the topic we're discussing today is that under the Privacy Act my organization has the authority to take complaints, to investigate, and to audit the personal information practices of more than 250 agencies and departments, including the RCMP, CSIS, and other national security agencies, such as FINTRAC.

Accompanying me today is Chantal Bernier, who is assistant commissioner for the Privacy Act. Madame Bernier was formerly assistant deputy minister in the Department of Public Safety and Emergency Preparedness. And with me as well is senior adviser Mr. Carman Baggaley, who accompanied me when I appeared before the inquiries of Mr. Justice O'Connor and Mr. Justice Major.

I believe all the honourable members have two documents that my office provided to you last week. The first piece is an overview, a backgrounder, of national security and surveillance laws passed in several countries since 2001, and it shows how much the social and political terrain has shifted dramatically after 9/11.

I'd like to talk a bit about how privacy laws apply to national security agencies.

In the various cases you were reviewing, this application is all too clear. The men who became the subjects of the inquiries that you were studying, as we just heard, suffered terribly, but as well as all the other harms they endured, the first violation was to their privacy.

To begin with, as Mr. Cavalluzzo has quoted, Justice O'Connor noted that inaccurate and misleading intelligence about them was compiled. That means their personal information, in terms of the Privacy Act, was shared inappropriately. Finally, this information was used to justify their detention, deportation, and subsequent torture.

[Translation]

Privacy rights under Canadian law are not simply about who is allowed to collect information. Privacy laws also set out who is accountable for protecting that information, ensuring it is accurate and limiting its disclosure to third parties. The findings of the O'Connor and Iacobucci reports call into question the practices of Canadian security agencies in all these areas. Both reports underscore how critical it is for officials in these departments to properly manage the collection, validation, sharing and careful review of the exchange of personal information.

[English]

Commissioner Iacobucci concluded in his inquiry that inaccurate information was collected on the individuals in question, that inaccurate information was shared with other states, and that safeguards for these files were not properly observed. Misleading, inaccurate, or out-of-date information was kept on file and shared too broadly, with few or no caveats on the use of that intelligence.

Privacy practices in government must be better defined, and sensitive information must be protected. This has never been more urgent than in light of the national security challenges we face. To address this question, the second piece that we have provided to this

committee presents our views on how oversight, privacy practices, and data protection in government could be improved.

[Translation]

While I have several suggestions for your consideration, if I can leave you with one over-arching message, it would be this—in an era of networked intelligence and surveillance, Canada needs a networked approach to oversight and review. Proper oversight and accountability for national security provide a vital check for Canadians' privacy rights.

[English]

In our recent history, rights and security are often pitted one against another. Margaret Bloodworth, who was Canada's former national security adviser, noted this tension just prior to her recent retirement. She said that safeguarding the privacy rights of citizens while also securing their physical security is not simply a question for the Canadian intelligence community, it is *the* question. It is the question, the single greatest issue that they must confront. I'd also add that security and privacy are not, as we often say, mutually exclusive. We need not, nor should we not in Canada, trade one for the other.

• (0925)

[Translation]

As you have heard from other expert witnesses, a fundamental question for national security in the 21st century is data governance. In a fully wired, networked world, how does any organization exercise quality control and oversight? Given the complexity of inter-agency, inter-jurisdictional, international, inter-sector intelligence operations—who can exercise that level of global review?

[English]

A recent report from the Office of the Auditor General in March 2009 on intelligence and information sharing stressed this point, that review bodies "must look beyond individual agencies to reflect the integrated nature of national security activities". These are the main points that I hoped to raise in our submission.

Now I'll just take you quickly through the recommendations. There are seven of them.

First of all, we recommend adopting an integrated approach to security review that allows for more coordination and more cooperation on investigations and reports across the system. This is the network approach recommended by Justice O'Connor. In my experience and in the experience of my office, this has worked to great effect. We do joint investigations with provincial privacy commissioners' offices. We do collaborative reporting with the Office of the Auditor General, for example. All of the review community, in my opinion, could benefit from similar powers.

000434

Second, I think we have to address the privacy practices within security agencies. The approach of departments and agencies to information sharing and data management has to change. Without proper attention to internal controls, new layers of oversight will not address front-line problems. Enhanced training around the theory and the practice of privacy, fair information practices, and data protection could affect great change here.

Third, appoint chief privacy officers across the government, but in particular for departments and agencies where collection of sensitive personal information is widely required by their mandate.

Fourth, provide the Commission for Public Complaints Against the RCMP with the resources and legal authority required to exercise more meaningful review. I believe Mr. Cavalluzzo has spoken quite completely to this question.

Fifth, request that the Treasury Board and ministers issue new policy requirements for departments and agencies on privacy. Robust information-sharing agreements through privacy impact assessments, well-developed privacy directions, and guidance must become part of how these organizations operate. We cannot have the informal, unstructured, and basically ungrounded sharing of information anymore.

[Translation]

Six, reform—as I have said before several other committees of the House of Commons—the Privacy Act, which dates back to 1983. In light of all that we have learned, I believe government departments must be held to a higher standard of privacy protection, information handling and data protection. I have recently put forward 10 “quick fixes” for government's consideration which could tighten controls on international information sharing, require departments to test the necessity of the information they collect and allow the Federal Court a wider role in reviewing violations of the act.

[English]

Seventh and finally, we urge Parliament to increase the resources and involvement of this House committee and its counterpart in the Senate. These bodies can provide active oversight of national security agencies and their operations. By pooling expertise, coordinating reviews, and sharing information, existing mechanisms for parliamentary review could be augmented.

Briefly, Mr. Chairman, I'd like to leave you with a few final thoughts.

While Canada's system of review and oversight functioned throughout the 1980s and 1990s, the stresses on the system after 9/11 have become tragically apparent. This needs to be addressed. When networks of intelligence sharing are global, oversight cannot remain rigid and localized. While I recognize that there's no silver bullet fix given these complex issues, I'm also keenly aware that there are very real human consequences that spring from poor information handling and governance. My office deals with them daily through our complaints process.

Thank you very much, Mr. Chairman, for your time and consideration. My office staff and I would be happy to answer your questions.

● (0930)

The Chair: Thank you very much for your opening statements.

We don't have much time, so we'll move immediately to the Liberal Party.

Mr. Holland, please, for seven minutes.

Mr. Mark Holland (Ajax—Pickering, Lib.): Thank you, Mr. Chair.

Thank you very much to the witnesses for taking the time to appear before committee today.

I'm going to start, if I could, with a real concern I have around information sharing. This was really a simple recommendation of Justice O'Connor's report, but what we have heard as we've gone through this process is really no assurance that anything has changed or that Justice O'Connor's recommendations have in fact been implemented.

Mr. O'Brien from CSIS was here and indicated that information was still being shared with countries with poor human rights records. We know that in Justice Iacobucci's report, he indicated that those same practices that were of such concern in the case of Mr. Arar were ongoing and continuing. We had a commitment from the minister stating that he would give a ministerial directive on sharing information with states that use torture, and that it would be forthcoming, and we haven't received it.

This is frustrating, because at the end of the day, the government's chief reason it gives is that we have the Air India inquiry going on, and they don't want to do anything until the Air India inquiry is complete. I'm just wondering if there is anything you feel that inquiry could possibly add to the recommendations already made on the caveats that should be in place with respect to Canadians sharing intelligence with countries that have poor human rights records, particularly countries that are known to torture.

I'll start with Mr. Cavalluzzo.

Mr. Paul Cavalluzzo: Just as a private citizen, I read somewhere where a government minister said that all of the recommendations in part one, which would include what you're talking about, have been implemented. I don't know if they have or haven't, but certainly as far as waiting for the Air India inquiry is concerned—and once again I'm speaking as a private citizen—I don't think it would be of assistance, as far as the issue you are talking about are concerned. What we're talking about here is dealing with countries with very poor human rights records, and realistically, as some witnesses have stated before us, in order to get information in respect of particular parts of the world we have to engage with partners that do not have great human rights records. If that's the case, then I think the decision to enter into that kind of a relationship should be a political one. It should not be made by a police agency or a security intelligence agency. I think that's a political question, and all Canadians should participate in that debate.

May 7, 2009

SECU-20

5

If we are going to have such a relationship, which realistically I think we have to, unfortunately, then we have to be very careful in terms of the information we send in respect of Canadians. We have to ensure that the information will not in any way be used in respect of human rights abuses. And in respect of information we receive from these agencies, we have to be realistic enough to know the public record, and the public record is that they engage in torture. If we get any information from these foreign agencies, we have to be realistic to understand that it's subject to torture and is likely unreliable, and we had better do a very good reliability assessment on it before we act on that information.

The kinds of issues I've just reviewed really are not part of the Air India inquiry, and there would be no need to wait for the recommendations of Justice Major to deal with those issues, which are very important.

Mr. Mark Holland: Before you respond, Ms. Stoddart, maybe I'll just add a couple of comments, to go into the recommendations you made, which I think are very good. Unfortunately a lot of them aren't new. We've seen a lot of them. So in the context of your response, could you address your recommendations and whether or not you feel there's any reason whatsoever that these recommendations should be held off for another inquiry?

I think Mr. Cavalluzzo made an excellent comment with respect to that. If a lot of these are implemented, particularly if the public complaints commissioner has the legislative power to actually be able to investigate, there won't be the need for all of these expensive inquiries that are going to be making the same conclusion.

Again, for the clarity of committee, on the recommendations you made, do you feel in any way that these have to be held back for another inquiry, such as the Air India inquiry?

• (0935)

Ms. Jennifer Stoddart: I think, as the honourable member pointed out, these are fundamental principles that are simply being reiterated and positioned for you, ideally, in the network world of modern intelligence sharing. I would think and hope that we could go forward with the necessary review and mechanism agency development without necessarily completely waiting for the results of another inquiry.

However, I would point out, because we appeared and made two submissions to the inquiry on Air India, that what it brings to this discussion is the fact that we have to look at the network world of security intelligence now, and we can't think it's just a matter of maybe the RCMP and the particular cases, and the two previous ones.

What we're also looking at in the Air India Inquiry, I believe, is how national intelligence infects—sorry, it should be “affects”, but perhaps “infects” in some way too—commercial domestic transport: the supervision of our airports, the supervision, for example, of airport personnel. So it brings into the picture the other agencies that are part of the national security world that I think we cannot ignore. And Transport Canada has a role to play. FINTRAC, which does money laundering review, is another part.

So I would say we have to be able to create a model that leaves a place for this kind of development. But I think my colleagues may have—

Mr. Mark Holland: Don't misunderstand me—and maybe you can just answer it this way—I think there's an important role for Justice Major to play and important recommendations for him to make. I just don't think the reiteration of the recommendations that you stated here or the reiterations of the recommendations we've heard as a constant refrain over the last four years are something we need to hear again to implement.

Would you agree that the recommendations you're making here and that we heard in Justice O'Connor's report, echoed in Justice Iacobucci's report, echoed in the pension scandal report, are things that we should go ahead and do, and that other things will come out of Justice Major's report that are separate and aside from this that we could act upon once we receive his conclusion?

Ms. Jennifer Stoddart: They may be separate and aside, but they're also connected, as I pointed out. Yes, we can go ahead, but we have to leave a place for the important recommendations and what will come out of that report.

Mr. Mark Holland: You wouldn't hold back going forward on these recommendations.

Ms. Jennifer Stoddart: I think they've been on the table for a long time.

The Chair: Thank you.

We'll move to Monsieur Ménard.

[Translation]

Mr. Serge Ménard (Marc-Aurèle-Fortin, BQ): Thank you, Mr. Chair.

Mr. Cavalluzzo, we were looking forward to meeting with you because we believe that you are familiar with the recommendations from Justice O'Connor and the reasons that led him to make them.

I understand that the part having to do with reparations for Mr. Arar was respected diligently. As far as we are concerned, the most important part of your recommendations deal with the future, recommendations that were made to avoid similar injustices occurring the future.

You have seen what the government has done since the tabling of your report. In this kind of recommendations for the future... We all recognize that not everything was done, but what is the most urgent thing that needs to be done?

[English]

Mr. Paul Cavalluzzo: I really can't comment whether the recommendations have been implemented. Once again, I'm speaking on my behalf as commission counsel and not on behalf of Mr. Arar. From my perspective, leaving aside part two, the most important recommendations he makes in part one relate to the two things I talked about.

One is information sharing. We see the effects of mislabelling individuals, particularly in foreign countries that are very aggressive as far as terrorist activities are concerned. Inaccurate information, once it's given, is very difficult to take away and remove from the file. Being called a terrorist today is like being called a communist in the 1950s. Once you're labelled a terrorist, it's very difficult to remove that description. On the information sharing, we have to ensure that there are policies in place to ensure the information is reliable and accurate, and that it complies with other laws.

The other important recommendation, which I discussed earlier and I think should be implemented as soon as possible, is the issue of the relationship between Canadian agencies and foreign agencies with poor human rights records. My own view is that any violation of human rights should be dealt with immediately. These are human rights. And if we're aware that foreign countries are abusing the rights of Canadians, we have to ensure and have in place policies that can deal with that situation—and effectively deal with that situation.

Unfortunately, in respect of Mr. Arar's case, there was a great deal of confusion, where different agencies of this country were acting at cross purposes. DFAIT was doing one thing, the RCMP was doing something else, and CSIS was doing something else. We need a coordinated and coherent approach when Canadians are being detained abroad. We have to implement these policies as soon as possible, because this is not a problem that is eliminated at this point in time, as we can see in respect of other situations that are going on today.

• (0940)

[Translation]

Mr. Serge Ménard: Concerning the first part, which deals with training for officers so that they use correct, precise and rigorous language, Mr. Zaccardelli assured us that training had been provided very quickly.

In our opinion, one of the major recommendations calls for broadening the authority of the agency that is responsible for oversight of the RCMP. In addition, it was recommended that this authority be exercised by an organization that would integrate more elements, an organization that would oversee the activities of the RCMP, the Canadian Security and Intelligence Service and other organizations.

Should such an organization also oversee the activities of the Department of Transport relating to risk management and the drawing up of a no-fly list? The Canada Border Services Agency needs to have security intelligence to manage both immigration and customs. I think that wasn't mentioned in the O'Connor report. Would you go as far as that?

A recommendation that an integrating organization be in charge of overseeing the activities of the RCMP, CSIS and other entities is certainly very important.

[English]

Mr. Paul Cavalluzzo: Yes, unquestionably, that is an important recommendation made by Justice O'Connor. He recommends that the new RCMP body also have jurisdiction over the CBSA, which was involved in the Arar case. SIRC, the Security Intelligence

Review Committee, would have jurisdiction not only over CSIS but also over Transport, CBSA, FINTRAC, and one other agency.

When a problem like Mr. Arar's occurs, Justice O'Connor foresees a complaint being filed with this new committee, and this committee would say, which body or bodies—because we have a number of Canadian entities involved in this—should review this situation? If you don't have review of some of these agencies involved in national security, then you're going to have an accountability gap. As lawyers say, you have to follow the trail, and the trail normally leads from agency to agency to agency.

[Translation]

Mr. Serge Ménard: Do you believe that we should wait for the report from the judge who is investigating the Air India attack before we establish these structures?

• (0945)

[English]

Mr. Paul Cavalluzzo: As a private citizen and not speaking on behalf Mr. Arar, I would note that Justice O'Connor delivered his last report in December 2006. We are now in 2009, and it seems to me that we have to act effectively. It's up to the government, but I have my own views on that.

The Chair: Thank you very much.

Mr. Davies, please.

Mr. Don Davies (Vancouver Kingsway, NDP): Thank you, Mr. Chairman, and thank you to all of the witnesses for appearing before us.

I think any right-thinking, rational person would agree that setting up an oversight body is required in this country. I think the efficacy of that depends on a number of factors, including who makes up that committee and how accountable the committee is to oversight, as well, to ensure that it doesn't conduct its own operations so secretly, or with such limitations, that it just becomes another layer of bureaucracy we can't puncture through.

So I want to know if anybody has any thoughts on the makeup of that committee, particularly whether it should be a mix of civilians and those with expertise. I guess what I'm driving at is civilian oversight. I wonder what you feel the civilian presence ought to be on such a committee. And do you have any comment on how we can make sure this oversight committee is responsible to Parliament, and ultimately to the citizens of Canada, to ensure that we ultimately get transparency and accountability through this structure.

Mr. Paul Cavalluzzo: Well, I think what is certainly recommended in the Arar report is that the overall coordinating committee in respect of national security be composed of the chair of the new RCMP body, the chair of SIRC, and the CSE commissioner, as well as an independent person who would chair the committee. That independent person, hopefully, would be someone who has a great deal of respect within the community, because as you say, transparency and accountability are important to these review mechanisms, particularly in the national security area. Those are the two important values.

May 7, 2009

SECU-20

7

As far as the individual bodies are concerned, I think SIRC is a good model for the new RCMP body. As we know, SIRC is composed of independent people who are normally former politicians or cabinet ministers with a great deal of public policy experience, who have the respect of the public; and as a result of that, what they do gains public confidence. The CSE commissioner is normally a former judge of the Supreme Court of Canada, who obviously has the respect of the community. So I think we need people like that who would gain public respect.

As far as legislative oversight is concerned, I think these bodies should be responsible to this committee, as well as to the Senate committee, on an annual basis, or on call by this committee when you feel something has to be reviewed, so that we have an independent arm of the executive responsible to a legislative committee and ultimately to Parliament, which is, of course, the parliamentary system in which we exist.

Thank you.

Ms. Jennifer Stoddart: Could I add to that, honourable member, that it's not just who's on the committee, who the committee reports to, but what the committee can do. What are its powers?

I think one of the reasons we have diagnosed that the public complaints committee against the RCMP has not been effective historically is that it depends on public complaints. I can echo that, because I also have complaint investigation powers, but if I only had that in terms of what I could do with my mandate, I would be a lot less effective.

So it is extremely important that this committee can take on initiatives, have audit power, compel production, and define the issues that are going to be reviewed by the committee.

I'll give an example of some of our recent work. In the federal government we have audit power. Following the beginning of the O'Connor inquiry, at about the time we appeared, we began a review of the RCMP exempt banks. Exempt banks are banks where people ask, am I in the bank? Is there a government file on me? And the RCMP don't have to answer. It is secret.

What we did find out in a special report we laid before Parliament was that the RCMP, in spite of what was going on in the Arar inquiry, had neglected to clean out these banks to see whether all these citizens.... There were I think thousands of innocent citizens who found themselves in these exempt banks and therefore possibly could show up on police files as people of interest, but they weren't allowed to know why they were in there.

My whole report was laid before Parliament, and I am sure the members are familiar with it.

But without that kind of power, you cannot go and look in the dark corners to see what might be hidden under the dust.

• (0950)

Mr. Don Davies: Thank you.

I'll probably direct this question to Mr. Cavalluzzo.

I worked with privacy legislation in my previous life. In my view, the main goal of privacy legislation is to ensure that our private information does not get disseminated improperly to people who

ought not to have it. But several times in the testimony I heard a reference to inaccurate, misleading information being disseminated and shared with other countries. What is particularly disturbing to me is that it is not normal, accurate information for which I have a privacy interest that was shared; it was inaccurate information. This was information given by our national police force. They are supposed to be professional investigators.

Can you comment on how that happened?

Mr. Paul Cavalluzzo: With the new anti-terrorism legislation the RCMP was given new national security responsibilities. You may recall that in 1981 the McDonald commission said the RCMP should get out of the national security game, and that is why we created CSIS. In any event, we brought them back into the national security game in 2001, and there was very little training for these front-line officers in national security issues.

As a result, these were good police officers, but they had no idea of the impact of the exchange of this kind of information, particularly with the Americans, and they had no idea that just because a piece of intelligence says this guy's neighbour says he's a member of al-Qaeda, you can't rely on that, that this is just information or intelligence. You have to analyze it, you have to corroborate it, and so on. Before you send any information like that, you'd better be sure it's accurate.

So for the most part it was really, unfortunately, a lack of training. I don't think there was any malfeasance, but certainly these people were not competent to be sharing that kind of information.

The Chair: We'll have to move to the government side now.

Mr. Rathgeber, please.

Mr. Brent Rathgeber (Edmonton—St. Albert, CPC): Thank you, Mr. Chair, and thank you to all the witnesses for your attendance today and for your expertise.

I find this topic quite fascinating and also very troubling, and I certainly share some of the concerns of my friend Mr. Davies. I too have some background with respect to freedom of information and protection of privacy. I chaired the review of the Alberta statute in the Alberta legislature.

Picking up on his question about inaccurate information, maybe this is just purely semantic or definitional, Ms. Stoddart, but I agree with his concern. Does personal information apply to information that is inaccurate? For example, I do not have a criminal record. If somebody were to disclose that I did, is that considered to be my personal information? Because it is not my personal information. It is wrong.

Ms. Jennifer Stoddart: You hit on a very important point there, honourable member. One of the bases of not only the Privacy Act but generally fair information principles is that the information about an individual has to be accurate. That individual, in democratic societies, has to have the right to have that information corrected. That's in fact a large part of what our office does.

What we see here are very particular cases of inaccurate personal information, unverified—and this is from the Iacobucci report and I believe the Arar report—being shared in a rather informal fashion. Again, it's not consistent with fair information principles about a very strict definition of the use to which you put personal information and accountability for the use of that personal information subsequently put.

This is one of the reasons that I think Privacy Act reform—Privacy Act applies to all the government agencies—is so important to give citizens a broader right to complain about inaccuracy of their personal information and, if the information is not corrected, to take it on to Federal Court. Right now, they don't have that right. It's a very truncated right. If they had had this kind of right, some of these cases may in fact have taken another turn of events.

• (0955)

Mr. Brent Rathgeber: Thank you.

In your opening comments, you quoted from Ms. Bloodworth, talking about privacy rights of citizens and ensuring physical security. You went on to make an interesting statement, that not only is this the greatest single issue that our Parliament must confront, but that security and privacy are not mutually exclusive.

I'm troubled by that concept. I certainly agree that both privacy and national security are invaluable goals that we must promote. But how can they not be mutually exclusive? I would suggest that in the unfortunate circumstance of Mr. Arar, an overzealous attempt to promote national security severely jeopardized and compromised his privacy rights and ultimately his human rights. In other situations, we could quote anecdotally that protection of privacy rights might have compromised national security.

I'm curious as to how they cannot be mutually exclusive, although I agree with you that they're both goals that ought to be zealously promoted.

Ms. Jennifer Stoddart: What I'm saying is that we don't have to continue to think about them as always being mutually exclusive. That's the challenge of the society that we live in. We have to protect our citizens. That's probably the number one role of government right now—physical security, integrity, safety. Those are basic human rights. Also, a basic human right is privacy, which means autonomy, which means freedom, which means our sense of liberty.

We have to organize, in our society, our processes and our laws in new ways to preserve them both so that one intrudes the least possible on the other. This is the challenge, because in the late 20th century Canada was fortunate in having a minimum of national security threats. Our privacy just came naturally because we were not a society under any kind of threat, compared to other societies where there were long histories of wars, invasion, persecutions, and so on. As we go forward, I am saying they are not in themselves, by nature, always mutually exclusive. That's what we have to aim to do.

Mr. Brent Rathgeber: I'm going to have to think about that a little bit more, but thank you.

Mr. Cavalluzzo, I read Justice O'Connor's report, or at least most of it, with great interest. I have a couple of questions on the creation of the independent complaint review committee.

First, why not just expand the role of the existing RCMP complaints committee, Mr. Kennedy's committee?

Secondly, I'm asking about your opinion or maybe his opinion vicariously through you. With all of these different committees—SIRC and the independent complaints review committee that Justice O'Connor recommends the creation of—how does that promote the coordinated and consistent approach you talked about? It appears to me that it's still a hodgepodge of different jurisdictions and different agencies.

Mr. Paul Cavalluzzo: Okay, in respect of Mr. Kennedy's committee, what Justice O'Connor talked about was a restructured CPC, so that the new independent review committee would have much broader powers than the CPC, including national security, as well as just general law enforcement powers, and that would be the new RCMP committee. So it's a restructured Kennedy committee, with much broader powers.

On the second point, in terms of coordination, the point once again of this new committee.... This isn't the RCMP committee, but there would be a broad coordinating committee, which would be composed of the chairs of the new RCMP body, SIRC, and the CSE commissioner, and national security complaints would be filed with this new coordinating committee. And the new coordinating committee would look at the complaint and say, "I think SIRC would be the body to deal with this", or he or she might say, "This involves the RCMP as well as CSIS, so I think both CSIS and the RCMP new committee should conduct a joint investigation." And certainly there would be new legislative gateways so that these bodies could act together, exchange information, and conduct joint investigations.

Where Justice O'Connor went to school, so to speak, on this is that there are foreign committees that conduct these kinds of joint investigations, and that way you have total control of the integrated investigation that has gone on, because there will be one committee acting—or could be acting— together that would cover all of the Canadians that are engaged in national security.

• (1000)

Mr. Brent Rathgeber: Thank you.

I suspect my time is done.

The Chair: Yes.

We'll move over to Mr. Oliphant now, please.

Five minutes.

Mr. Robert Oliphant (Don Valley West, Lib.): Thank you.

And thank you, again, for being with us today.

With all due respect to my colleagues across the way, without wanting to get into a sermon, I wanted to quickly raise three points.

May 7, 2009

SECU-20

9

Despite having read the report...this report is simply not about sharing of information in general that may be government information; this is about sharing wrong information, misleading information, inaccurate information, and damaging information that has hurt people's lives. Recommendation after recommendation in Justice O'Connor's report is about people who are Canadians.

That falls into my second point, which is that not only are privacy and security not mutually exclusive, they're intimately bound together and cannot be released from each other. We are not safe if we do not have the ability to have our privacy protected. We have a false sense of security. It's not that they're possibly not mutually exclusive; they are absolutely entwined with each other or our Canadians are not safe.

That's the end of my sermon. Excuse me. Amen. I want to preach.

I'll get to my question. The bulk of this report is about privacy and information. The bulk of the recommendations have to do with information and inaccurate sharing of information. That puts us into the concept of labelling and what happens when people are labelled, which is bad enough, but when we share the labelling with either agencies within this country or, worse, outside this country with partners who are not dependable, we have a huge problem. And the report is very clear, in recommendation 5 I think it is, that the minister should be issuing ministerial directives to ensure that labelling does not take place by the RCMP or any of the other agencies that are involved in this.

Are you aware of any ministerial directives that have been released since 2006—we're now in 2009—since this report was issued?

Mr. Paul Cavalluzzo: I am not, but that doesn't mean it hasn't happened. I'm in private practice now, doing other things, and so I'm not aware of whether such a directive has been issued. Certainly there was a recommendation that it be issued, but I'm not aware of it.

Ms. Jennifer Stoddart: Yes, I'm aware, and I'd ask maybe Mr. Baggaley if he could talk to this.

I believe Treasury Board is working on a directive of this kind, because members of my staff have been consulted.

Mr. Carman Baggaley (Strategic Policy Advisor, Office of the Privacy Commissioner of Canada): What I wanted to comment on was that Justice Iacobucci specifically raises the issue that you referred to. In fact, one of his findings is to suggest that in fact it's a practice to send information to another country labelling someone as an Islamic terrorist, or something else, as a kind of fishing expedition to determine whether or not the receiving country can either confirm or deny that allegation. Although Commissioner Iacobucci doesn't make any recommendations in his report, as you may know, he comes very close to suggesting a recommendation, and he strongly disapproves of that type of practice where it's done deliberately. It's not being done because they're not quite sure, but according to the justice, it's being done as a kind of fishing expedition.

Mr. Robert Oliphant: My concern is that the labelling practices that we became aware of as a result of O'Connor and Iacobucci continue to this day, and this is affecting my constituents. They and their families are labelled when they try to cross the border and when they're met by CSIS agents, who want to interrogate them about

issues constantly. It's a practice that I think is extremely dangerous for our security. I think it's intimately related to our security, because if one Canadian is not safe, we're not safe as a society.

It seems to me that the Office of the Privacy Commissioner has to constantly be vigilant on this issue, as you are, but what else can we as a committee do to help you do this work that we value so greatly? You're suggesting we have more resources to do our work; what else can we do to be supportive of you and to protect Canadians?

• (1005)

Ms. Jennifer Stoddart: By raising the issues and by raising interest in the various aspects of privacy—and there are many—parliamentary committees in the last few years have helped to make Canadians much more aware of their privacy rights and how they can be improved, so we certainly appreciate your attention to the issues and the recommendations that come out of the various committees. For example, our own ethics committee on Privacy Act reform would have an impact on the issues we're discussing here, because one of the things I hope they recommend is to put in a necessity test for collecting information. This is a basic principle of fair information—principles around the world. If there had been a necessity test applied to the use of the collection of information by national security agencies, we might have another story today.

The Chair: Thank you.

Mr. McColeman, please go ahead.

Mr. Phil McColeman (Brant, CPC): I want to thank all of you for coming and sharing your expertise. Certainly the depth of knowledge is extensive here, and we're learning a lot in trying to move towards doing the right thing by protecting public safety while balancing the rights of individuals.

Although it really wasn't the direction I was going to go in, I'm interested in following up on the commissioner's comment on the necessity test.

You said earlier that the first violation was the violation to their privacy, if I might paraphrase what you were saying. What is the test of crossing the line on privacy? Is this the necessity test that you just referred to?

Ms. Jennifer Stoddart: There are many components of fair information, which is part of our privacy. Our privacy can have many dimensions, but in terms of information about us, you go through the sequence of how the information circulates about us. One of the fundamental principles is that an organization collects only the information it needs, not just any information it can Hoover up, any information it might find about you that it would keep just in case it could be useful some day. The principle is to collect only the information that is actually needed, because it is actually your private information.

Then we go on to other principles, such as the requirement for the information to be accurate and up to date. You only share it for purposes that are, as our own Privacy Act says, consistent; that is, they're roughly equivalent, or they're compatible with, the reason for which it was initially collected.

All this is to prevent government agencies or the government itself from turning us into a surveillance state that has all kinds of information on individual Canadians that it can't justify.

Mr. Phil McColeman: I appreciate where you're going on this continuum of a police state in which we collect too much information on individuals, but let me suggest something to you and get your reaction.

Part of my experience was on an oversight body for police services in my community. The reality in a lot of situations is that because we are human, there's going to be human error, and this human error is going to mean that sometimes bad things happen that shouldn't happen to people. That's unfortunate. I'm not diminishing any of the reports that have come out, but I'd like you to address that and assist this committee in terms of your thinking on this continuum, because the collection of information, the determinations, and the judgments made as to whether we should go down this road or another road are all subject to errors by individuals and to human error along the way.

I don't think we can have a playbook saying that if this happens you do this, and if this happens you do that. What are your thoughts as to where you strike this balance or determination on where you head with information?

• (1010)

Ms. Jennifer Stoddart: Could I ask Assistant Commissioner Bernier, who is a specialist on the Privacy Act, to answer?

Ms. Chantal Bernier (Assistant Privacy Commissioner, Office of the Privacy Commissioner of Canada): I would say that it is precisely the reality of human error that begs for oversight, review, remedies for correction. As the commissioner said before, privacy rights include the right to accurate information as well as the right to have inaccurate information corrected, so your own statement is precisely the basis for the necessity of proper oversight mechanisms, which is what we are putting forward.

Mr. Phil McColeman: I'll probably have time for one last question here.

We had representation from the British Parliament on their oversight mechanism for national security. Are you familiar with that model? This is one whereby the Prime Minister appoints senior parliamentarians, people who really have no agenda to move through the political process, because as you can see from our interaction here, things become politicized very easily at this level. In a serious matter such as national security, I wish it weren't that way, frankly. I speak for myself here.

Having said that, the British model is one in which these parliamentarians operate in a fairly secretive environment. They get the very details of what has happened and have to be sworn to secrecy on a lot of these matters. They're hand-picked by the Prime Minister and report to the Prime Minister of Britain.

What do you think of that model?

Ms. Chantal Bernier: I am familiar with it and in fact have had the privilege of meeting them as well.

We have discussed it at the OPC. We feel that its transferability to Canada must be assessed by the competent authorities. If such a proposal were to be put forward, we would obviously look at it through the lens of the Privacy Act. We do not have a position at this stage.

Mr. Phil McColeman: That's interesting. Thank you.

The Chair: We'll have to wrap it up there.

Monsieur Ménard.

[Translation]

Mr. Serge Ménard: Thank you.

It's funny, but at the very end, if I had had the time, I would have asked the question that my colleague just asked. Perhaps I could talk to you about this right now.

The O'Connor report does not contain any suggestions in this regard. Even so, there was a bill tabled by Ms. McLellan of the previous government, which was intended to set up this kind of committee. Since then, nothing has happened.

Concerning the questions from Mr. Oliphant, I think it is essential for us to categorize people that police officers are investigating. Be it investigations into organized crime or more of an investigation relating to national security, when the police suspect people, it is important for the other police forces to know that these people are under suspicion. Even if the police officers do not yet know whether the suspicions are justified or not, suspects must be categorized when criminal intelligence is being analyzed.

For example, we talked about persons of interest. In my opinion, Mr. Arar was one. However, there are thousands of people of interest who are not terrorists. If we met them under other circumstances, or if we observed them, we could verify if there was something else that could justify taking them from the "person of interest" category and placing them in the "suspect" category, or moving them from the "suspect" category to the "confirmed person" category or the "people we are sure of" category.

I would like to hear Ms. Stoddart's opinion on this. In my opinion, such categories should remain secret, because if the person has been put in the wrong category, and if we want investigations to go somewhere, we must not let people know that they have been slotted into a particular category and are under investigation. Such suspicions can be passed on to other countries or to agencies of other countries.

Ms. Jennifer Stoddart: In my opinion, you have raised an important issue, namely, the type of categorization that both the police and people working in national security need to do. The message that I would like to give you today is not that any type of categorization is prohibited under the Privacy Act, far from it. It is absolutely essential that our security forces do this type of classification. The problem that we have raised and which results in a contravention of the Privacy Act and in a breach of citizens' rights occurs when categorization is inaccurate and false.

May 7, 2009

SECU-20

11

I will go back to my example of the review we did pertaining to the RCMP's exempt data bank, which existed at the same time that the Arar Commission was doing its work. If we had not had the authority to audit that exempt bank, there would have been all kinds of inaccurate audits, and the name and identity of several thousand Canadians would have ended up in an exempt data bank, because these individuals would have been persons of interest to the RCMP. When we began our audit, the RCMP was the first to admit that this data bank had not been cleaned up. It's possible—and we were not able to ascertain whether or not this was the case—that there were repercussions for individuals whose name had been in this bank for five or six years at the time of the audit.

I completely agree with you that we need to move persons from one category to another, but this has to all be based on facts.

• (1015)

Mr. Serge Ménard: One thing we can certainly agree on is that it's also important that rigorous practices be adopted, not only to ensure people's safety but also to protect them from unfair suspicions. That's what was missing in the Arar case, which, as we well know, had a disastrous outcome. I believe that in the other three cases as well, the process lacked rigour from the outset.

Ms. Stoddart, I would like to know your opinion of the practice of disclosing the legal files of Canadian citizens to other countries. In your opinion, should we be readily sharing citizens' legal files, using the quickest methods available, like the computer? If not, what precautions should be taken before such disclosures are made?

[English]

The Chair: Please be very brief.

[Translation]

Ms. Jennifer Stoddart: Under the terms of the Privacy Act, there has to be an agreement or an arrangement. In the work that my office has been doing in the area of national security, we have noted that, over the past five years, there often has not been clearly defined parameters. Rather, we have seen informal exchanges whereas the legislation more or less says that the agreement needs to clearly define what can be exchanged and why. Informal exchanges that happen on the spur of the moment, without any forethought, can pose serious privacy risks.

[English]

The Chair: Thank you.

We'll go to Mr. Richards now, please, for five minutes.

Mr. Blake Richards (Wild Rose, CPC): Thank you. I appreciate your being here today.

Obviously privacy issues are very important; privacy is one of the important rights that we as Canadians enjoy. Of course, we have to balance this right with others, such as the right to safety and security. I'm sure you're well aware of that. I appreciate the detail and the thought you've put into some of the recommendations you've brought forward to us today.

Of course, when we look at recommendations such as these, we always have to be mindful of the costs involved. When I say that, I talk about not only financial and logistical costs, but also the opportunity cost. As an example, for every minute that the RCMP

spends on paperwork or ensuring that we're not unduly invading anyone's privacy, there is an opportunity cost to it; it gives away some of their time that could be spent investigating. We always have to be mindful to make sure we find the right balance.

That's where I want to go with my questions to you. I'm sure someone who has put as much thought and detail into recommendations as you has certainly thought about those logistics and the costs, including opportunity costs, involved.

I will point to just a few of the recommendations in your report: talking about requiring within security agencies enhanced training around the theory and practice of privacy; appointing chief privacy officers across government; providing the Commission for Public Complaints Against the RCMP with the resources required to deal with privacy issues; talking about the Treasury Board and ministers issuing new policy requirements for their departments, especially around thorough privacy impact assessments; talking about increasing the resources of committees such as this one and the Senate committee. These things all have costs, be they financial costs or opportunity costs.

I'm wondering how much thought you have put into what kind of new resources would be required to implement these recommendations and how much these recommendations would cost, and whether you have thought about their implications in terms of balancing privacy with other activities that these bodies and agencies can and should be doing as well. Give me a bit of a sense as to what you see the cost here being, in terms of resources, finances, and also opportunity costs.

• (1020)

Ms. Jennifer Stoddart: Okay.

Mr. Blake Richards: I know that's a broad question to ask. Maybe you want to focus on one or two of the recommendations I've indicated.

Ms. Jennifer Stoddart: Yes, thank you.

Mr. Chairman, my office isn't really equipped to evaluate the cost of these various recommendations. I believe the Treasury Board is.

Perhaps the point I could make to this committee is that the opportunity costs are the important factor to look at. If we had invested in, for example... Mr. Cavalluzzo mentioned that in 2001 the RCMP, having been out of national security, all of a sudden—whoops!—came into the field, and the people were not trained. If they had been trained in information management practices and if there had been a chief privacy officer, perhaps much of the saga that in the end was very costly to the Canadian public might have been avoided.

I think my colleague wants to briefly add something.

Ms. Chantal Bernier: I would submit to you, first of all, that we need to talk about or at least consider the cost of not doing it.

Secondly, we know, for example, that since the advent of the Charter of Rights and Freedoms, we have seen that the added rigour that consideration for human rights brings to police investigations has, indeed, added a gain in efficiency both in terms of cost and opportunity, as you suggest.

Mr. Blake Richards: Could you give me some examples of how that is in fact the case? I'm not disputing that it is, but—

Ms. Chantal Bernier: For example, a police officer will not inundate himself or herself or a file with unnecessary information, but will be much more focused, that focus perhaps being initially brought on by considerations for privacy, but leading to a much more efficient investigation process.

Mr. Blake Richards: I'm not disputing what you're saying at all, but there are always two sides to the story. That could be true, and I think it may very well be, but there also could be the other side of it: that sometimes it may be they're spending time being concerned about ensuring privacy, and this takes away some of the information they could have used in an investigation.

The Chair: We'll have to wrap it up there. I'm sorry. We have eight minutes left. Can we split it—four minutes and four minutes?

Mr. Kania, go ahead.

Mr. Andrew Kania (Brampton West, Lib.): Madam Stoddart, in your May 7, 2009, submission, "Rights and reality: enhancing oversight for national security programs in Canada", you indicated that "The recommendations from the O'Connor Policy Review have yet to be implemented". Are you aware of the fact that the government takes the position that they have all been implemented except for the overall supervisory organization?

I have a quote here. As far back as when Stockwell Day was the public safety minister, he indicated, in responding to Commissioner Iacobucci's report, that O'Connor's recommendations have, in fact, all been implemented. He also stated that there had been considerable progress towards designing a new model for review, on which there would apparently be a public announcement in the near future. That was when Stockwell Day was public safety minister.

I'm wondering if you have seen any evidence of any implementation of any of the three recommendations.

Ms. Jennifer Stoddart: I am aware of the differences of opinion between my statement and the government statements. That's from our various perspectives, I being a parliamentary watchdog agency.

What I mean is that the recommendations have not been fully implemented, and we do not see them being operational. We do not see any kind of oversight and review committee, which is the main focus of my message to you today.

I am aware, however—and I think in that sense it explains the government's position on this—that work is being done on this. Work is being done within the government. I mentioned that we had been consulted on draft directives for more appropriate information sharing within the government. We also have been told that work is being done within Public Safety Canada on an oversight committee.

Indeed, my colleague, who was there until six months ago, can speak to that.

• (1025)

Mr. Andrew Kania: You would all presumably agree with me that when former Minister of Public Safety Stockwell Day indicated, quite some time ago, that all the recommendations were implemen-

ted, that would not have been accurate. Would you all agree with that comment?

Ms. Jennifer Stoddart: I have not seen all the recommendations from the O'Connor inquiry implemented, some of which had to do with a committee that I don't believe is in existence.

Mr. Paul Cavalluzzo: I think we have to be cautious here. I don't know if Minister Day was talking about part one. If he was talking about part one, then perhaps all those recommendations have been carried out. As far as part two is concerned, clearly that hasn't happened.

We have to look at the context of his statement as to what he was talking about.

Mr. Andrew Kania: Let's discuss that. Obviously part two has not been implemented. We all know that.

Mr. Paul Cavalluzzo: That's correct.

Mr. Andrew Kania: In terms of part one, do you have any proof or evidence that they have been implemented?

Mr. Paul Cavalluzzo: No, other than the statement of a cabinet minister, and I would rely on that statement.

Mr. Andrew Kania: Other than that individual's statement, there's nothing else you have.

Mr. Paul Cavalluzzo: That's correct.

Mr. Andrew Kania: Let's assume, because we see no evidence that they've been implemented, that they've not been. Are you aware of any new cases or rights abuses that have taken place since these reports?

What I'm trying to get at is that these recommendations have not been implemented. Obviously they were made to prevent further abuses. As a result of the failure to implement, are you aware of any other cases that have arisen?

Ms. Jennifer Stoddart: I would simply say that we do have ongoing complaints against many organizations with national security mandates, but I do not know...and the nature of our regime is that I can't speak of the contents publicly. Certainly we have complaints on an ongoing basis against many of the organizations we've discussed today.

The Chair: Thank you very much.

We'll go to Mr. MacKenzie, please.

Mr. Dave MacKenzie (Oxford, CPC): Perhaps you can see why the British system might not work as well here as it does in Britain.

Is that not the nature of your work, to investigate ongoing complaints?

Ms. Jennifer Stoddart: Yes, absolutely.

Mr. Dave MacKenzie: If we go back to the Air India inquiry that's ongoing, one of the issues raised in that was the lack of information sharing between the federal agencies, and so on. Are there things we can learn and should learn and perhaps have learned from that particular inquiry in a public sense of why we need to improve information sharing among our agencies as opposed to limiting it?

May 7, 2009

SECU-20

13

I understand the need for privacy, but I think there is a need for sharing.

Ms. Jennifer Stoddart: Yes. I don't disagree with that.

I can't prejudge what Mr. Justice Major may be saying in his report; however, I did find very instructive the recent report of the Auditor General, which I think is very illuminating on this question and which highlighted the need for intelligence sharing. Highlighted also was the fact that some recommendations she made in an audit in 2003, I believe, had not been followed up on.

Highlighted also was the misuse of the Privacy Act, which is a great concern of mine, in that the Privacy Act is quoted as a reason for not sharing intelligence among national security agencies. When the Auditor General asked where the legal opinion was or where the memorandum was and how they analyzed the Privacy Act such that they thought it prevented them from sharing information, there were none of these documents.

I think that's an important part of the puzzle that we have to look at. It's not only that the Privacy Act be respected, but possibly that the Privacy Act be refocused to be more contemporary, and also that it not be used wrongly as a shield against necessary information sharing.

• (1030)

Mr. Dave MacKenzie: One of the witnesses before the Major inquiry who was from the Canadian banks, which are mandated to provide information through FINTRAC, indicated, I think, that there was an issue about their feeling that they were in the dark. They must provide the information, but there's no sort of feedback, if you will, or whatever.

There's a sense that there's a big package there that is worthwhile, and that it is worth their time and effort to do it, but that sometimes we get caught up—and rightly so—in being concerned about privacy. Sometimes we make it so secret that the folks whose cooperation we need in a general sense feel that perhaps we've gone too far one way.

I don't know whether you have any comments.

Ms. Jennifer Stoddart: I think my colleague has some thoughts on that.

Ms. Chantal Bernier: Indeed, as the commissioner has said, we would refer you to the March 2009 Report of the Auditor General, wherein she specifically raises that issue and says that the Canadian population will trust the national security and intelligence organizations only if it knows that they have maintained the proper balance between privacy and national security. She goes on to say that this proper balance has not been struck due to a lack of guidance to the departments and agencies concerned.

I can tell you what we are doing at the moment in this regard. You've mentioned FINTRAC. We are about to complete an audit of FINTRAC. We are mandated by law to do so, and it is about to come out, so you will certainly want to turn your attention to that.

In 2006, we did an audit of CBSA. We are following up on it now and we are addressing, in that context, information sharing agreements. We are also working with Treasury Board, as my colleague Carman Baggaley and the commissioner have said, on developing guidance on information sharing. This guidance will contain provisions on transborder sharing of information.

Finally, we are also reviewing the very recent Transport Canada-RCMP agreement on information sharing from the point of view of privacy.

Mr. Dave MacKenzie: I think that at one point you were perhaps going to answer my colleague across the aisle when there was an issue about whether anything had been done, and I think Ms. Stoddart indicated that in your previous home you perhaps had more knowledge about how some of those things may have been done.

I know that we simply don't have the time, but I'm quite satisfied that it isn't the case that nothing's been done; there has been a great deal done. Maybe it's not complete, but there has been a great deal done, and I know it's through the work of people like you, so thank you.

Ms. Chantal Bernier: Thank you.

The Chair: I'd like to thank the witnesses. We'll end this portion of our meeting. We're going to suspend for a minute or two.

Again, thank you very much. We're going to have to clear the room because we're going in camera.

[Proceedings continue in camera]

Published under the authority of the Speaker of the House of Commons

Publié en conformité de l'autorité du Président de la Chambre des communes

**Also available on the Parliament of Canada Web Site at the following address:
Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante :
<http://www.parl.gc.ca>**

The Speaker of the House hereby grants permission to reproduce this document, in whole or in part, for use in schools and for other purposes such as private study, research, criticism, review or newspaper summary. Any commercial or other use or reproduction of this publication requires the express prior written authorization of the Speaker of the House of Commons.

Le Président de la Chambre des communes accorde, par la présente, l'autorisation de reproduire la totalité ou une partie de ce document à des fins éducatives et à des fins d'étude privée, de recherche, de critique, de compte rendu ou en vue d'en préparer un résumé de journal. Toute reproduction de ce document à des fins commerciales ou autres nécessite l'obtention au préalable d'une autorisation écrite du Président.