Privacy Commissioner of Canada
Commissaire à la protection de la vie privée du Canada

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

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.

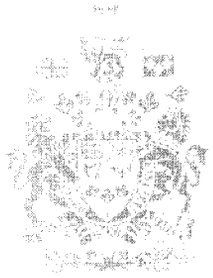
We are concerned that clause 16 of Bill C-52 would give authorities access to a wide scope of personal information without a warrant; for example, unlisted numbers, email account data and IP addresses. The Government itself took the view that this information was sensitive enough to make trafficking 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.

.../3



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.

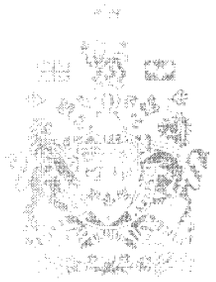
We appreciate your consideration of these concerns.

Sincerely,

Jennifer Stoddart,
Privacy Commissioner of Canada

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

.../5



Elizabeth Denham,
Information and Privacy Commissioner for British Columbia

Irene Hamilton,
Ombudsman for Manitoba

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

Ed Ring,
Information and Privacy Commissioner for Newfoundland and Labrador

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

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

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

.../6

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

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

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.