



House of Commons
Chambre des communes

Honourable Vic Toews
Minister of Public Safety
House of Commons
Ottawa, ON K1A 0A6

Re: Omnibus Crime Legislation and Lawful Access Legislation

June 24, 2011

Dear Minister Toews,

At the outset, let us congratulate you on your re-election and your reappointment as Minister of Public Safety for the new Conservative government. We are writing over our concern about elements of the upcoming omnibus crime legislation that could seriously erode the privacy rights of Canadian citizens. Specifically, we are concerned with bills drafted in the 40th Parliament – Bills C 50, 51 and C-52 that together comprise “Lawful Access” legislation.

The New Democratic Party supports legislation to ensure that police have the powers to address the emerging threats posed through cyber crime. We support efforts to bring policing into the digital age. However, a number of provisions in this legislation, if left unamended, would seriously erode the privacy rights of ordinary citizens.

Of particular concern is Clause 16 of the former Bill C-52 allowing security services unrestricted access to any device identification data from an ISP or other telecommunications service provider without a warrant. This will allow law enforcement to identify individuals involved in a striking array of online activity including anonymous political opinions made in blog posts or newspaper comments, location data posted online from a smart phone, social networking activity, private online instant message or email exchanges, and a host of currently unforeseeable future online interactions that are sure to come with new innovations and services. This unrestricted access to e-mail addresses will make it possible to track individuals across a vast range of online services, activities, and even locations.

Clause 16 will enable widespread use of tracking by unique mobile device identifiers. No studies have been done on the implications of these surveillance capabilities (as was highlighted in a recent report of the Ontario Privacy Commissioner on WiFi device identifiers). Such identifiers are persistent across devices, can be collected in new and unexamined ways such as through smart phone application interfaces, and can often be linked to real time location data.

This creation of a digital panopticon where every action of a citizen can be tracked and scrutinized is unprecedented. What is even more disturbing is the fact that the bill does not limit in any way the reasons for which an officer or other security official might make such a demand.

... / p. 2



Needless to say, Privacy Commissioners from across Canada have expressed serious concerns about such a provision. In an unprecedented move, they have written a challenge to the government:

“...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...by enhancing the capacity of the state to conduct surveillance and access private information while reducing the frequency and vigour of judicial scrutiny.”

Clause 17 of Bill C-52 allows for police to gain access to such information without the need for prior judicial approval in any circumstances where that information is immediately necessary to prevent a crime or serious harm. Clause 16, however, goes much further, by allowing law enforcement to gain information on Canadians where they have no reason to suspect the information will be useful in any way. If passed as is, the question will not be whether abuse will occur, but how widespread such abuse would be.

Allowing security services to engage in unchecked fishing expeditions on private citizens will certainly put individual rights and liberties at risk. How is it possible for a democratic country to consider it beneficial to allow the state to obtain personal information where there is no reason to suspect the information will be useful to an investigation? I refer you to the letter from the Privacy Commissioners of Canada in their direct challenge the government to produce evidence of the need for such sweeping changes:

“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.”

This expansion of e-surveillance powers is all the more troubling given the lack of any effective oversight mechanisms put in place by this legislative regime. Bill C-52 in particular relies heavily on external audit powers granted to the Office of the Privacy Commissioner of Canada with respect to the warrantless disclosures it puts in place. As noted by the Privacy Commissioners of Canada, these oversight powers are insufficient and largely replicate mechanisms already available in the federal *Privacy Act*. Oversight must be expanded in breadth and scope if it is to have any alleviating effect, and it must be accompanied by sufficient funding and resources to permit the Privacy Commissioners to carry out their objectives.

A further concern arises from the impact some of the operational requirements that the legislation will have on the security of our communications as well as on online innovation. The bill will require online service providers to build spyware backdoors into their services as well as the ability to provide decrypted communications.

Such spyware interception requirements have raised serious security issues in countries such as Greece, for example, where criminals exploited backdoors of this nature to spy on Greek government officials. The operational and decryption requirements in bill C-52 are especially troubling as they appear to go

even further than those in analogous U.S. legislation, and may have detrimental impacts on cross-border interoperability of online telecommunications services using end-to-end encryption to ensure secure conversations.

Another element of deep concern is in Sub-Clause 6(2) which, for example, allows the Government to impose a gag order on telecom service providers that will prevent them from telling their customers that personal data is being intercepted. The current definition of "telecommunications service provider" is murky and so broad that it could capture a wide range of online telecommunication services including blogs, social networking sites, search engines and even online newspapers as long as these services use a telecommunications facility such as a server in the provision of their services. The lack of clarity on this issue is an example of the need for careful study at Parliamentary committee to ensure that there are not unintended consequences on the development of the digital economy.

A final concern is the disproportionate impact some of Bill C-52's requirements are likely to have on smaller ISPs and mobile service providers and, consequently, on their ability to compete in Canadian markets. Will smaller ISPs and mobile service providers be expected to meet the same standards for surveillance as large competitors? This legislation will impose added costs on equipment upgrades that smaller service providers will have difficulty meeting. The compensation for warrant-less information requests will burden small service providers with the obligation to respond to all manner of requests, spurious or otherwise. Given the existing lack of competition in the market, has the government given any consideration to the implications of adding such burdens on emerging ISP and mobile players in the telecom market?

On the much broader level, the implications of such a move are breathtaking. It would force commercial Telecom services to become an extension of the surveillance arm of the state. Canada's Privacy Commissioners rightly characterized this unprecedented departure from existing principles:

"We are concerned that the proposed powers are not limited in any fashion... We believe that there is insufficient justification for the new powers, that other, less intrusive alternatives can be explored and that a focused, tailored approach is vital. In our view, this balance has not been achieved."

Such a fundamental rewiring of the internet infrastructure appears to contravene the Canadian Charter of Rights and Freedoms. Section 8 specifically provides citizens with the right to be protected from "unreasonable search and seizure." How will the government justify widespread snooping of consumer use of the internet without the consent of consumers and without clear limitations on the use of these powers?

In 2007, former Justice Minister Stockwell Day made a clear commitment that any new legislation regarding cyber policing would respect the longstanding norms of judicial oversight. "We have not and we will not be proposing legislation to grant police the power to get information from Internet companies without a warrant. That's never been a proposal," stated Minister Day.

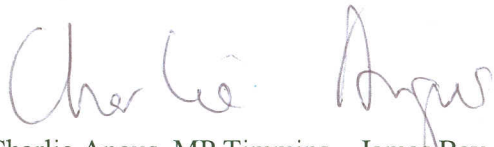
Will your government honour this commitment?

As none of these proposals have undergone parliamentary scrutiny, will you commit to ensuring that the ‘Lawful Access’ provisions of the omnibus crime bill will be set apart so they can undergo full review by Parliamentary committee?

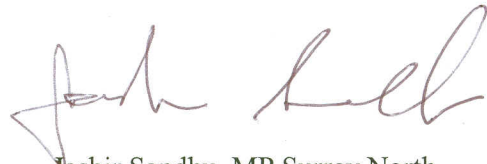
Minister, we are sure you will agree that the complexity of the issues raised in terms of policing in the cyber environment requires legislation that is responsive to changing policing needs while ensuring that the longstanding rights of citizens to privacy are respected.

We look forward to hearing from you in this matter.

Yours,



Charlie Angus, MP Timmins – James Bay
NDP Ethics, Privacy and Digital Issues Spokesman



Jasbir Sandhu, MP Surrey North
NDP Public Safety Critic