



PUBLIC INTEREST ADVOCACY CENTRE

LE CENTRE POUR LA DEFENSE DE L'INTERET PUBLIC

ONE Nicholas Street, Suite 1204, Ottawa, Ontario, Canada K1N 7B7

Tel: (613) 562-4002. Fax: (613) 562-0007. e-mail: piac@web.net. <http://www.piac.ca>

October 18, 2007

BY E-MAIL ONLY

Customer Name and Address Consultation

Public Safety Canada

16C, 269 Laurier Avenue West

Ottawa, ON

K1A 0P8

Dear Madam or Sir:

I am writing you on behalf of the Public Interest Advocacy Centre (PIAC) to comment on the "Customer Name and Address Information Consultation" document.¹ To date there have been three such consultations (2002, 2005 and now 2007) by successive governments regarding what also has become known as "Lawful Access".

PIAC is concerned that the Consultation document is short and undetailed in comparison to past materials supplied (sometimes in confidence) regarding what appears to be an identical initiative. Indeed, the Consultation document is so short as to be misleading to the uninitiated. The only real detail provided is two potential justifications for the entire regime – emergency notification and investigative "bootstrapping".

Regarding these two justifications for the warrantless collection and use of "customer name and address information", generally we endorse the criticisms of and questions raised by the response to this consultation made by the Canadian Internet Policy and Public Interest Clinic (CIPPIC).

Regarding emergency situations, we note in addition that PIPEDA already provides an exception for use and disclosure of personal information in a situation that is life-threatening or likely to result in serious bodily harm to an individual, without consent. Although we appreciate that some telecommunications companies may believe they require a warrant for even this sort of access, it is in fact permitted to be used to respond to the emergency by the holder of the information (see PIPEDA, s. 7(2)(b)) or may indeed be disclosed to law enforcement or others in an individual emergency (see PIPEDA, s. 7(3)(e)). The only complication is that the holder of the information that is disclosed must immediately notify, in writing, the subject of the personal information about the disclosure. However, if an emergency is the real purpose for the request, authorities should not take issue with notification to the individual. To the extent that telecommunications providers are reticent about disclosure of personal information in a true emergency situation, it would seem a simple matter of education about the PIPEDA exception.

¹ "Customer Name and Address Information Consultation" Document, Online: <http://securitepublique.gc.ca/prg/ns/cna-en.asp>

Warrantless investigation, however, appears to be the larger goal of this consultation. Nothing appears to have changed from the previous consultations: PIAC assumes that what was presented to the few stakeholders who were invited to the consultations mentioned in the Consultation document (we were not) was that the standard for access will be a non-judicial one (where police or other “authorized persons” simply demand the information from telecommunications service providers due to “suspicion” that a subject (or group of subjects) is somehow involved in an undefined or somewhat defined list of “offences”). If we are mistaken in this assumption, we assume that at the least, if any judicial oversight is indeed required, that it will be on less than a “reasonable to believe” standard (the standard for most present wiretap authorizations – although there is also a “reasonable to suspect” standard for certain offences). This is implied by the wording of the Consultation document that reads in salient part:

For example, law enforcement agencies may require the information for non-investigatory purposes (e.g., to locate next-of-kin in emergency situations) or because they are at the early stages of an investigation. The availability of such building-block information is often the difference between the start and finish of an investigation. [Emphasis added.]

Assuming there is a framework being contemplated that is roughly what has been proposed the last two times, we refer you to PIAC’s 2002 comments on “Lawful Access”,² much of which address the warrantless standard and the civil liberties protected by the *Canadian Charter of Rights and Freedoms* in relation to privacy and search and seizure. It appears the same flaws, from PIAC’s point of view, exist in this initiative, with the exception that none have been explicitly addressed in this consultation – which begs the question whether it is deliberately or just negligently obfuscatory.

PIAC further views the CNA information sought to be collected as clearly personal information, either under legal interpretations of various privacy commissioners and courts, or the opinion of the public.³ Therefore the Minister’s statements to the press that: “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,” and “It may make some investigations more difficult, but our expectation is rights to our privacy are such that we do not plan, nor will we have in place, something that would allow the police to get that information”⁴ should not be based on a semantic game if it is an attempt to define CNA as something other than “information” or to suggest it is not private in this context.

Should the government wish to troll through online personal information without judicial oversight, or under a greatly reduced standard of judicial oversight, it should at the least be subject to serious public oversight (by Parliament and the general public), there should be severe penalties for misuse of the information and its collection and use should be restricted to only highly serious and defined offences.

Yours truly,

Original signed

John Lawford
Counsel

2 See Public Interest Advocacy Centre, Comments on the Federal Government’s “Lawful Access” Consultation Document (December 16, 2002). Online: http://www.piac.ca/files/piac_dec16_02.pdf

3 See PIAC, “Consumer Privacy and State Security: Losing Our Balance” (November 2004) at p. 29, where it is noted that 86% of Canadians in a POLLARA poll indicated they expect government to get a warrant to read their e-mail or monitor their web-surfing habits. Online: <http://www.piac.ca/files/statesecurity.pdf>

4 See CBC News Online, “Day firm on police warrants for access to internet user data” Online: <http://www.cbc.ca/canada/story/2007/09/14/tech-privacy-warrant.html>