

CUSTOMER NAME AND ADDRESS (CNA) INFORMATION CONSULTATION DOCUMENT

INTRODUCTION

Modern telecommunications and computer networks such as the Internet are a great source of economic and social benefits, but they can also be used in the planning, coordination, financing and perpetration of crimes and threats to public safety and the national security of Canada. By extension, the rapidly evolving nature of these technologies can pose a significant challenge to law enforcement and national security officials who are entrusted with combating these threats, and who employ lawful access to communications and information to do so.

The principles and powers of lawful access must be exercised in a manner consistent with the rights and freedoms guaranteed in the *Canadian Charter of Rights and Freedoms* and while adapting to the rapid pace of technological change.

THE CONSULTATION PROCESS

Public Safety Canada, in collaboration with Industry Canada, is presently examining how to address the challenges faced by police, the Canadian Security Intelligence Service (CSIS) and the Competition Bureau when seeking timely access to basic CNA information in a modern telecommunications milieu. This question was previously considered by stakeholders in broader consultation processes on lawful access issues held in 2002 and 2005.

The purpose of this consultation is to provide a range of stakeholders - including police and industry representatives and groups interested in privacy and victims of crime issues - with an opportunity to identify their current views on possible approaches to updating Canada's lawful access provisions as they relate to law enforcement and national security officials' need to gain access to CNA information in the course of their duties. The possible scope of CNA information to be obtained is later identified, but it should be noted from the outset that it would not, in any formulation, include the content of communications or the Web sites an individual visited while online.

The objectives of this process are to maintain lawful access for law enforcement and national security agencies in the face of new technologies while preserving and protecting the privacy and other rights and freedoms of all people in Canada. In striving to attain these goals, it is essential to ensure that the competitiveness of Canadian industry is taken into account and that the solutions adopted do not place an unreasonable burden on the Canadian public.

CURRENT CONTEXT

Timely access to CNA information is an important tool used by law enforcement and national security agencies to fulfil their public safety mandates. This type of information can be vital in the context of investigations of online criminal activity, such as child exploitation.

Law enforcement agencies have been experiencing difficulties in consistently obtaining basic CNA information from telecommunications service providers (TSPs). In the absence of explicit legislation, a variety of practices exists among TSPs with respect to the release of basic customer information, e.g., name, address, telephone number, or their Internet equivalents. Some companies provide this information voluntarily, while others require a warrant before providing any information, regardless of its nature or the nature of the situation. If the custodian of the information is not cooperative when a request for such information is made, law enforcement agencies may have no means to compel the production of information pertaining to the customer. This poses a problem in some contexts. 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.

CNA INFORMATION

In the context of options under consideration by Public Safety Canada and its partner departments and agencies, CNA information refers to basic identifiers that would assist law enforcement and national security agencies to determine the identity of a telecommunications service subscriber, if this information was necessary to the performance of their duties.

The scope of CNA information obtained could include the following basic identifiers associated with a particular subscriber:

- name;
- address(es);
- ten-digit telephone numbers (wireline and wireless);
- Cell phone identifiers, e.g., one or more of several unique identifiers associated with a subscriber to a particular telecommunications service (mobile identification number or MIN; electronic serial number or ESN; international mobile equipment or IMEI number; international mobile subscriber identity or IMSI number; subscriber identity module card number or SIM Card Number);
- e-mail address(es);

- IP address; and/or,
- Local Service Provider Identifier, i.e., identification of the TSP that owns the telephone number or IP address used by a specific customer.

POSSIBLE MODEL

Options based on an administrative model are being considered closely by officials.

POSSIBLE SAFEGUARDS

Further to input received during 2002 and 2005 consultations, a number of safeguards could be included under a possible administrative model requiring the release of limited basic CNA information to law enforcement and national security agencies upon request. These could include:

- clear limitations on what customer information could be obtained upon request;
- limiting the number of employees who would have access to CNA;
- requiring that individuals with access be designated by senior officials within their organizations;
- limiting requests to those made for the purpose of performing an official duty or function;
- requiring that requests be made in writing, except in exceptional circumstances;
- requiring that designated officials provide associated information with their request, e.g., identification of a specific date and time for a request relating to an IP address;
- requiring designated officials to record their status as such when making a request, as well as the duty or function for which a particular request is made;
- limiting the use of any information obtained to the agency that obtained it for the purpose for which the information was obtained, or for a use consistent with that purpose, unless permission is granted by the individual to whom it relates;
- requiring regular internal audits by agency heads to ensure that any requests for CNA information are being made in accordance with the protocols and safeguards in place;
- reporting to responsible ministers on the result of any internal audits;

- provision of any audit results to the Privacy Commissioner of Canada, the Security Intelligence Review Committee, or provincial privacy commissioners, as appropriate; or
- provision for the Privacy Commissioner and SIRC to conduct audits related to the release of CNA information.

Under no option being examined would TSPs be compelled to track the actions of customers or to collect information about them in the absence of necessary court authorizations governing such activity in Canada, nor would law enforcement or national security agencies be permitted to obtain the content of a customer's communications without such authorizations.

CONCLUSION

Officials plan to meet with a range of interested parties in September, 2007 to discuss the issues raised in this paper.

Written comments may also be sent to the following address by September 25, 2007, and will be gratefully received:

Customer Name and Address Consultation
Public Safety Canada
16C, 269 Laurier Avenue West
Ottawa, ON, Canada K1A 0P8