Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

Customer Name and Address (CNA) Information Consultation Document

Response of the Office of the Privacy Commissioner of Canada to Public Safety Canada

October 2007
Ottawa, Ontario

Jennifer Stoddart
Privacy Commissioner of Canada

The Rationale for the Consultation

According to the consultation document issued by Public Safety Canada and Industry Canada, "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."[1]

The consultation document is based on the assumption that law enforcement and national security (LE/NS) agencies are experiencing difficulties obtaining access to customer name and address (CNA) information in a timely way. The consultation document sets out the problem as follows:

> 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.

The excerpt above suggests that the problem is one of inconsistency; some TSPs provide this information voluntarily while others are unwilling to provide this information or will do so only in response to a warrant.

The consultation document states "This poses a problem in some contexts" and it goes on to refer to two situations where problems arise. The first involves the use of CNA information for non-investigative emergency purposes; the second involves the use of CNA information during the early stages of an investigation.

Unfortunately the consultation document does not provide any sense of the scope of the difficulties mentioned in the document. Are 80 per cent of TSPs providing CNA information voluntarily or is the figure 20 per cent? Are telephone companies more likely to provide the information than Internet service providers (ISPs)? Are small TSPs more likely to request a warrant? Nor does the consultation document indicate whether TSPs respond differently depending on the situation. For example,

[1] The consultation document is available at http://securitepublique.gc.ca/prg/ns/cna-en.asp

do TSPs respond differently to next-of-kin emergency situations than they do to requests involving suspected violent crimes?

Requiring all TSPs to disclose CNA information on request is an overly broad, one size fits all response to a problem that has not been clearly defined or measured. We raised this issue in response to the 2002 consultation and the 2005 consultation on lawful access:

> When the 2002 Consultation Paper on Lawful Access was issued by the Department of Justice, Industry Canada and the Solicitor General, our Office, along with several other parties, questioned the need to revise the existing lawful access regime. We pointed out that the departments had failed to demonstrate the existence of a serious problem that needed to be addressed. We urged the three departments to present a clear statement of the problems that law enforcement agencies were encountering along with empirical evidence supporting the need for enhanced surveillance powers proposed in the consultation paper.
>
> This has still not been done. Without a clear understanding of the problems that the proposed legislation is intended to correct it is impossible for our Office or the Canadian public to determine if the measures being proposed are necessary and proportionate.

Although the current consultation addresses only some of the issues raised in previous consultations, the comments we made in 2005 are still appropriate.

The *Personal Information Protection and Electronic Documents Act (PIPEDA)*

As federal works, undertakings and businesses (FWUBs) all TSPs operating in Canada are subject to *PIPEDA* even if they only provide service in a province with substantially similar legislation.

PIPEDA requires that organizations obtain consent for disclosures of personal information subject to a limited number of exceptions. Three of the exceptions are particularly relevant to the issues raised in the consultation document:

- Under paragraph 7(3)(c) an organization may disclose information without consent when it is required to comply with a subpoena, a warrant or a court order;
- Under paragraph 7(3)(c.1), an organization may disclose personal information to a government institution, including a law enforcement agency, for the purpose of enforcing a law, carrying out an investigation, gathering intelligence for the purpose of enforcing a law, or administering a law; and
- Paragraph 7(3)(e) allows disclosures without consent to a person who needs the information because of an emergency that threatens the life, health or security of the an individual.

Paragraph 7(3)(c) deals with mandatory disclosures pursuant to a legal authorization.

Paragraph 7(3)(c.1), in contrast, is clearly intended to allow organizations to disclose personal information without consent or notification to LE/NS agencies and other government bodies in the absence of prior judicial authorization. However, the organization requesting the information has to identify its legal authority and indicate that it is collecting the information for one of the reasons listed in the paragraph, for example to enforce a law of Canada, a province or a foreign jurisdiction.

When the legislation (Bill C-6) was being debated in the House of Commons, the Minister of Industry clearly stated that 7(3)(c.1) was intended to maintain the *status quo*, "These amendments do not grant new powers to government institutions, nor do they create new obligations on business." Although 7(3)(c.1) was not intended to alter the *status quo* we appreciate that it may have created some uncertainty on the part of organizations being asked to disclose certain information.

This provision was the subject of a considerable amount of discussion during the mandatory five year review of *PIPEDA* conducted by the House of Commons Standing Committee on Access to Information Privacy and Ethics. In its report, tabled on May 2, 2007, the Committee recommended that consideration be given to clarifying what is meant by 'lawful authority' in section 7(3)(c.1). The Committee also recommended changing the "may" in the opening paragraph of subsection 7(3) to "shall" which seemingly would have made all the disclosures in 7(3) mandatory.

In its response to the Committee's report, table on October 17, 2007, the government indicated that there is a need to clarify the concept of lawful authority. The government rejected the Committee' recommendation about changing "may" to "shall."

The government's response also sought to clarify the overall intent of the paragraph:

> The government wishes to confirm that the purpose of s. 7(3)(c.1) is to allow organizations to collaborate with law enforcement and national security agencies without a subpoena, warrant or court order. Organizations who share information with government institutions, including law enforcement and national security agencies, in accordance with the requirements of this provision, are doing so in compliance with *PIPEDA*.

The government also indicated that it will examine the possibility of adding a regulation to further define the term "government institution" that is found in 7(3)(c.1) and 7 (3)(d).

Although neither the Committee's report nor the government's response directly referred to 7(3)(e), the government's response stated that it would consider certain limited exceptions to *PIPEDA*'s consent requirements to address the concerns expressed by stakeholders regarding the disclosure of personal information in cases

of natural disasters, elder abuse and other similar circumstances. Such a change would undoubtedly be relevant to the issue of disclosing CNA information to LE/NS agencies for emergency purposes.

As the consultation document suggests, at least some of the difficulties that LE/NS agencies face in terms of obtaining CNA information is one of inconsistency. The changes that the government is proposing to make to *PIPEDA* as a result of the five year review may go a long way towards clarifying when and how TSPs may disclose CNA information under 7(3)(c.1) and possibly 7(3)(e).

The Privacy Commissioner has stated publicly that she would not object to adding definition for the terms "lawful authority" and "government institution" if the government feels that such definitions would bring clarity to the legislation.

Although the consultation paper identifies the "absence of explicit legislation" as one of the problems the consultation process seeks to address, *PIPEDA* is, in fact, an explicit legislative code that permits lawful access by LE/NS agencies while "preserving and protecting the privacy and other rights and freedoms of all people in Canada." Before considering legislation that would make the disclosure of CNA mandatory on request, we would strongly recommend that the government determine if the clarification to *PIPEDA* discussed above, together with any guidance that may be appropriate, address the inconsistency. In terms of guidance, Service Alberta has produced a guidance document, "Requesting Personal Information from the Private Sector: Forms and Guidelines for Law Enforcement Agencies", that includes two forms that law enforcement agencies can use when requesting personal information from organizations.[2]

CNA and the Expectation of Privacy

The Consultation document does not define CNA information, but it states that it 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 of SIM Card Number);
- e-mail address(es);
- IP address; and/or,
- Local Service Provider Identifier (LSPID), i.e., identification of the TSP that owns the telephone number or IP address used by a specific customer.

[2] See http://www.pipa.gov.ab.ca/resources/pdf/forms_and_guidelines_for_law_agencies.pdf

Referring to all of this information as customer name and address information is misleading, as is calling these data elements "basic identifiers." This list goes well beyond the customer names and addresses associated with a given telephone number. Some of this information is available through white page directories and reverse directories. However, much of this information is not publicly available; furthermore, much of this information would be unknown to the individuals involved. For example, many people with Internet service do not know their IP address. Similarly, many cell phone subscribers would not even know that there are any identifiers associated with their telephone other than the number.

The assumption behind the consultation paper is that CNA information carries a low expectation of privacy and as such does not require judicial authorization. We disagree: many individuals consider much of this information to be private. First of all, a significant number of people choose to pay extra for unlisted telephone numbers, demonstrating that they consider these numbers to be private. Many people only share their cell phone numbers with friends and family numbers. One of the attractions of the Internet is that it provides an expectation of privacy. Many people use pseudonyms on the Internet in order to engage in anonymous communications and for a variety of other reasons.[3]

In *BMG et al v. John Doe et al* Justice von Finckenstein concluded that it would irresponsible for the Court to order disclosure of the name of an account holder given the uncertainty that exists about the link between the identity of an account holder and an anonymous user as well as the link between the user of an account and a given dynamic IP address. [4]

While some of the this information might be considered less sensitive we need to recognize that it is typically not being sought as an end in itself. CNA information may be valuable to LE/NS agencies specifically because it can provide access to even more sensitive information.

Section 8 of the Charter of Rights and Freedoms protects Canadian against unreasonable search and seizure when there is a reasonable expectation of privacy.

---

[3] See Wilkins J. in *Irwin Toy Ltd. v. Doe* (2000), 12 C.P.C. (5th) 103 (Ont. Sup. Ct.) at paragraphs 10-11: "Implicit in the passage of information through the internet by utilization of an alias or pseudonym is the mutual understanding that, to some degree, the identity of the source will be concealed. Some internet service providers inform the users of their services that they will safeguard their privacy and/or conceal their identity and, apparently, they even go so far as to have their privacy policies reviewed and audited for compliance. Generally speaking, it is understood that a person's internet protocol address will not be disclosed. Apparently, some internet service providers require their customers to agree that they will not transmit messages that are defamatory or libellous in exchange for the internet service to take reasonable measures to protect the privacy of the originator of the information."

[4] *BMG Canada Inc. v. John Doe* [2004] 3 F.C.R. 241.

The Supreme Court has recognized that an individual's expectation of privacy may depend on location, the nature of the information and the relationship of the information to the individual. On the third point, one criterion the Court uses in deciding if an individual has a reasonable expectation of privacy is whether the personal information involves "a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state".[5]

In *R v. Plant*, where this concept of "a biographical core of personal information " was first used, the Court found that electricity consumption records did not meet this biographical core test. One consideration used by the Court in reaching this conclusion was that this information is generally accessible by the public. This is not the case with unlisted numbers and cell phone numbers which are fiercely protected by many people indicating a strong expectation of privacy.

In a strong dissenting judgment in *R. v. Plant*, Justice McLachlin (as she then was) noted that

> [c]omputers may and should be private places, where the information they contain is subject to legal protection arising from a reasonable expectation of privacy. Computers may contain a wealth of personal information. Depending on its character, that information may be as private as any found in a dwelling house or hotel room.[6]

Many, if not all, of the various types of personal information included within the ill-named category of "customer name and address" information constitute personal information to which a reasonable expectation of privacy attaches. We strongly recommend that due consideration be given to the *Charter* implications of any legislation that would make it mandatory for a TSP to disclose this personal information when confronted with a warrantless request that is, in reality, a demand.

Proposed Safeguards

The paper proposes a number of safeguards that could be implemented if the government decided to require TSPs to disclose CNA information on request. However, these safeguards only become relevant if one accepts that mandatory disclosure is an appropriate and necessary solution.

We do not propose to comment on the proposed safeguards in any detail. We will comment more fully on possible "checks and balances: and oversight models if legislation is introduced implementing these proposals.

The consultation paper suggests that agency heads be required to conduct regular internal audits to ensure that any requests for CNA information are being made in accordance with the protocols and safeguards in place. The paper goes on to

[5] *R. v. Plant*, [1993] 3 S.C.R. 281.
[6] *Ibid.*, para. 45.

suggest that audit results be submitted to the Privacy Commissioner of Canada, the Security Intelligence Review Committee, or provincial privacy commissioners, as appropriate.

The paper also refers to explicit provisions to allow the Privacy Commissioner and the Security Intelligence Review Committee to conduct audits related to the release of CNA information.

While after the fact audits are an important means of assessing compliance, they are not a substitute for prior authorization. With respect to our ability to conduct audits with respect to the disclosure of CNA information, our Office can conduct a compliance review of a government department or agency at any time at the discretion of the Commissioner under section 37 of the *Privacy Act*,. Under section 18 of *PIPEDA* we require "reasonable grounds to believe" that an organization is contravening the Act before we can conduct an audit. Although some provincial commissioners may have the authority to audit a provincial or municipal police force in terms of compliance with provincial privacy legislation they do not all have this authority, or the resources to conduct such a review. It is not apparent how the federal government could require a provincial or municipal police force to maintain audit records. This would potentially leave a significant gap in terms of oversight.

Conclusion

The consultation paper is based on a number of assumptions:

1. LE/NS agencies are experiencing difficulties in obtaining access to CNA information that are sufficiently serious to justify new privacy intrusive measures;
2. there is no reasonable expectation of privacy in CNA data;
3. requiring TSPs to disclose this information on request is necessary to address these difficulties; and
4. this approach preserves and protects "the privacy and other rights and freedoms of all people in Canada", as the consultation paper suggests.

We are not convinced that these assumptions are sound. First of all, we do not have a clear sense of the seriousness of the problem. Neither this consultation paper nor previous consultation documents has presented a compelling case based, on empirical evidence, that the inability to obtain CNA in a timely way has created serious problems for LE/NS agencies in Canada. This calls into question the policy rationale from both a proportionality and necessity perspective. Second, it is our view that a reasonable expectation of privacy attaches to CNA data. This renders any mandatory disclosure/seizure regime of dubious constitutional validity.

Assuming there is a well documented and empirically demonstrated problem in obtaining access to CNA information, we are not convinced that requiring TSPs to disclose this information without a warrant is the only solution or the most appropriate solution. As discussed above, clarifying *PIPEDA* and providing guidance, may go a long way towards resolving this matter. We would also point

out that the Canadian Radio-television and Telecommunications Commission (CRTC) has already addressed the issue of access to provider information (LSPID) by law enforcement agencies in Telecom Decision CRTC 2002-21[7]. In that decision the CRTC determined in order to obtain LSPID, a law enforcement agency had to identify its lawful authority to obtain the information and indicate that

1. it has reasonable grounds to suspect that the information relates to national security, the defence of Canada or the conduct of international affairs;
2. the disclosure is requested for the purpose of administering or enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing or administering any such law; or
3. it needs the information because of an emergency that threatens the life, health or security of an individual, or the law enforcement agency otherwise needs the information to fulfill its obligations to ensure the safety and security of individuals and property.

The CRTC's decision uses language similar to that found in subsection 7(3) of *PIPEDA* with the significant addition of the reference to "reasonable grounds to suspect". The CRTC's approach should also be considered.

Finally, we agree with the consultation paper that "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*." However, we are not convinced that allowing LE/NS agencies to obtain CNA information on demand would meet this threshold. As discussed above, we do not accept the premise that individuals have a low expectation of privacy with respect to the information in question and that obtaining this information without judicial authorization would protect "the privacy and other rights and freedoms of all people in Canada."

[7] Telecom Decision CRTC 2002-21, 12 April 2002, Provision of subscribers' telecommunications service provider identification to law enforcement agencies.