Canadian Internet Policy and Public Interest Clinic
Clinique d'intérêt public et de politique d'internet du Canada

Philippa Lawson
Director
(613) 562-5800 x2556
plawson@uottawa.ca

October 15, 2007

BY EMAIL AND MAIL

Public Safety Canada
16C, 269 Laurier Avenue West
Ottawa, ON
K1A 0P8

Dear Sir/Madam:

Re: Customer Name and Address Consultation

1. The Canadian Internet Policy and Public Interest Clinic ("CIPPIC") is a legal clinic based at the University of Ottawa, Faculty of Law. CIPPIC's mandate includes intervening in legal and policy-making processes on issues arising from the use of new technologies, the outcomes of which have broad public interest implications. Our goal is to ensure that important public interest voices are heard in the policy-making process so that results reflect more than strong vested interests.

2. Public Safety Canada, in collaboration with Industry Canada, has initiated a public consultation on the issue of "updating Canada's lawful access provisions as they relate to law enforcement and national security officials' need to gain access to CNA [Customer Name and Address] information in the course of their duties."[1]

3. The following are CIPPIC's comments in response to the Consultation Paper.

Background

4. The government's Consultation Paper sets out law reform proposals that closely reflect those proposed by the Liberal government two years ago in Bill C-74, the *Modernization of Investigative Techniques Act*, which died with the 38th Parliament when an election was called shortly thereafter. An identical bill was later introduced by Liberal M.P. Marlene Jennings as a private member's bill (Bill C-416), but this bill also died on the order paper when Parliament was prorogued.

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

5. The proposals to give law enforcement agencies easier access to basic information about telecommunications subscribers have been mooted by the federal government for a number of years. In 2002, the Canadian government announced plans to modernize its criminal law and establish new rules regarding "lawful access" in light of the challenges posed by new technologies to law enforcement. That year, the government consulted with stakeholder groups, including civil society, on a number of ideas including the creation of a national CNA database. Over 300 submissions were received, many from individuals and organizations concerned about the potential impact of the proposals on privacy and civil liberties.

6. In early 2005, government officials initiated targeted, closed consultations with stakeholders (including industry and civil society) on revised proposals, having taken into account the input received in earlier consultations. The revised proposals included "warrantless" access to CNA information.[2]

7. In both sets of consultations, civil society raised serious concerns about the impacts of the proposals on the privacy and civil liberties of individuals, and expressed opposition to proposals for warrantless access to subscriber data. CIPPIC has summarized the consultations and views expressed by civil society in a webpage located at http://www.cippic.ca/projects-cases-lawful-access/. This webpage also includes links to written submissions and other relevant documents.

8. Bill C-74, the *Modernization of Investigative Techniques Act*, was introduced in November 2005. Among other things, the bill included provisions requiring telecommunications service providers to hand over certain subscriber identifying information to law enforcement agencies upon request, without any need for reasonable grounds to suspect criminal activity and without a court order, warrant, or other judicial authorization. The bill did not get past First Reading before an election was called.

9. The current Consultation focuses on essentially the same proposal for warrantless access by law enforcement agencies to customer name and address ("CNA") information from telecommunications service providers.

10. According to the most recent consultation paper, "[t]he 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," while ensuring "that the solutions adopted do not place an unreasonable burden on the Canadian public."

The Problem

11. The proposals in question are designed to address problems currently being experienced by law enforcement agencies. The Consultation Paper explains the problem as follows:

[2] By "warrantless access", we mean the right to demand and obtain such information without a warrant, court order, or other judicial authorization, and without reasonable grounds to suspect criminal activity.

> 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.

12. The problem thus seems to have two distinct aspects:
    a) locating next of kin in emergency situations, and
    b) gathering CNA information during the early stages of an investigation.

Locating next-of-kin in emergency situations

13. With respect to the former, the appropriate solution is to require that TSPs hand over the necessary information upon request *for the purpose of locating next-of-kin in an emergency situation*; it is not to allow police to demand such information for the much broader purpose of "performing an official duty or function". Especially where fundamental civil liberties are at stake (see below), solutions should be tailored to the problem at hand.

Gathering CNA information in early stages of investigations

14. The second aspect of the problem, as stated in the Consultation Paper, is more troubling. It is not clear whether the problem here involves situations where:
    a) the police *have* reasonable grounds to suspect criminal activity but need to act immediately and don't have time to obtain a warrant;
    b) the police *have* reasonable grounds to suspect criminal activity but simply don't want to go through the process of obtaining a warrant; or
    c) the police lack reasonable grounds to suspect criminal activity and therefore *can't* get a warrant to obtain the information.

15. In the first situation, section 487.11 of the *Criminal Code* allows police to engage in searches without a warrant "if the conditions for obtaining a warrant exist but by reason of exigent circumstances it would be impracticable to obtain a warrant." Presumably, the problem here is that the police can't obtain the information in question without the cooperation of the TSP, and some TSPs are not cooperating. As with the emergency situation described above, this situation can and should be addressed with provisions tailored to the problem in question. Thus, if the problem is that TSPs are refusing to hand over subscriber information regarding someone the police have reasonable grounds to believe is engaging in criminal activity, and if the urgency of the matter justifies proceeding without a warrant, then the proposed law should permit the police to demand production of information where such criteria are met.

In practical terms, the police officer requesting the information from the TSP should be required to communicate the grounds for the request to the TSP, as well as to record it for audit purposes.

16. If police simply want to be relieved of the administrative effort of obtaining warrants for CNA information in cases where they *have* reasonable grounds, we again submit that the proposed solution is too broad. First, it is not clear how the public will benefit by relieving the police of due process requirements in cases that do not involve exigent circumstances. More evidence of how due process requirements regarding CNA information are currently impeding legitimate investigations is needed before mandating disclosure without a warrant requirement. Second, as noted below, CNA information, especially in the digital context, is much more than mere "tombstone" data. It can open the door to a host of detailed information about the individual. We therefore see no reason to apply a lower threshold for access to CNA information than to other information about subscribers.

17. Assuming, however, that there is good reason to relieve police of the warrant requirement for CNA information (as opposed to other information) where they *have* reasonable grounds to suspect criminal activity, then once again, the proposed solution is too broad. Binding requests for CNA information should be limited to those made for the purpose of investigating suspected criminal activity where the requestor has reasonable grounds to believe that a crime is being, has been, or will be committed. Even if third party authorization is not required, "reasonable grounds" can be required and police can be held accountable after the fact. As noted above, the police officer making the request should be required to state the grounds for the request to the TSP, and to record it along with relevant evidence for audit purposes.

18. If, on the other hand, the problem is that the police want to be able to gather CNA information when they have *no* reasonable grounds to suspect criminal activity, we submit that the proposal is unacceptable. Such requests, in our view, constitute "fishing expeditions" and violate fundamental principles of due process. In free and democratic societies, police should not be engaging in proactive investigations without any reasonable grounds to suspect criminal activity. To allow such investigations is to invite abuse. We doubt that it would withstand a *Charter* challenge. Our laws of due process have been carefully crafted so as to balance police powers with civil liberties. Allowing what amount to forced searches without any requirement for reasonable grounds to suspect criminal activity would upset this balance.

Definition of "lawful authority" in subs.7(3)(c.1), PIPEDA

19. Although not stated in the Consultation Paper, we understand that there is another problem underlying the proposal for easier access to CNA information. According to law enforcement agencies and victim rights advocates, some TSPs demand warrants before handing over CNA information because they interpret subs.7(3)(c.1) of the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") as requiring such

authorization.[3] PIPEDA contains a number of exceptions to the general rule that organizations must not disclose information about identifiable individuals (including CNA information) without consent. These exceptions include the following:

> *(c)* [where] required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;
>
> (*c*.1) [where] made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that
>
> > (i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,
> >
> > (ii) the disclosure is requested for the purpose of 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 any such law, or
> >
> > (iii) the disclosure is requested for the purpose of administering any law of Canada or a province;

20. The term "lawful authority" in subs.7(3)(c.1) is not defined in the Act. Apparently, it is being interpreted by some TSPs as requiring authorization in the form of a warrant, court order, or other judicial authorization.[4] Hence, some TSPs consider themselves prohibited from disclosing CNA (and other personal) information to the police unless the request is accompanied by a warrant.

21. It is our understanding that this interpretation was not intended by the drafters of PIPEDA or by Parliament when it passed PIPEDA. Subs.7(3)(c) already provides for disclosures in response to warrants, court orders, etc. Subs.7(3)(c.1) was added in order to preserve the *status quo*, under which organizations were free to disclose personal information to law enforcement agencies even without any warrant or other formal authorization. The term "lawful authority" was meant, we believe, to refer to the institution's authority, not to due process requirements. Although we support those organizations that choose not to disclose other than in response to warrants, it is our understanding that PIPEDA gives the organization discretion to make that choice; it does not prohibit such disclosures.

22. To the extent that the problem underlying these proposals stems from this misinterpretation of subs.7(3)(c.1) of PIPEDA, we submit that the appropriate response is to define "lawful authority" in PIPEDA. It is not to substantially change the law so as to remove the discretion of organizations to demand warrants before handing over their subscribers' identifying information.

---

[3] See Submissions and Testimony of the Canadian Chiefs of Police and the Canadian Resource Centre for Victims of Crime to the House of Commons Standing Committee on Access to Information, Privacy and Ethics in its review of PIPEDA, Meeting No.30, Feb.13, 2007, online: <http://cmte.parl.gc.ca/Content/HOC/committee/391/ethi/evidence/ev2695445/ethiev30-e.htm#Int-1895029>

[4] Hereinafter, we use the term "warrant" to cover all forms of court orders or judicial authorization.

Reasonable expectations of privacy in CNA Information

23. According to the consultation paper, the proposals are designed to assist law enforcement and national security agencies in determining the identity of telecommunications service subscribers, and "would not, in any formulation, include the content of communications or the web sites and individual visited while online." The CNA information in question "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, i.e., identification of the TSP that owns the telephone number or IP address used by a specific customer.

24. If this proposal were to go forward, it is essential that the scope of information subject to the new rules be highly constrained (certainly, no broader than in this proposal) and not subject to expansion in future years. This is best done by including the definition in legislation, not ancillary regulations.

25. However, the proposal for warrantless access to CNA information is questionable insofar as it is based on the premise that CNA information attracts a lower expectation of privacy than does other (e.g., message header or content) information associated with individuals. While names and addresses may *generally* attract a lower expectation of privacy than do other types of personal information, that is not necessarily true - especially in the electronic context. Names and addresses can be keys to a host of sensitive personal information such as financial records and health details, much of it available by simple internet searches. As some commentators have noted, allowing unfettered access to CNA information:

> …will bestow upon law enforcement officials a reservoir of personal information from which to fish. These deep basins will allow officials to cast their nets wide, enabling access to personal information that reveals core biographical data…. *typical subscriber information of the sort made available under the proposed … scheme will become the means by which a biographical core of personal information is assembled* .[5]

[5] Daphne Gilbert, Ian R. Kerr and Jena McGill, "The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers," (2007) *Criminal Law Quarterly*, vol. 51(4) 469 at 502-503 [citing, in part: Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York: New York University Press, 2004)].

26. Many people use pseudonyms on the Internet in order to engage in anonymous communications without fear of embarrassment or retribution. They have a high expectation of privacy in relation to their Internet identities, and reasonably so. Unmasking their identities without any kind of judicial authorization or requirement for reasonable cause to suspect criminal behaviour is not consistent with the values of a free and democratic society, and may indeed violate the *Canadian Charter of Rights and Freedoms*.[6]

Charter implications

27. Section 8 of the *Canadian Charter of Rights and Freedoms* provides everyone with "the right to be secure against unreasonable search and seizure."[7] According to the Supreme Court of Canada, s.8 protects people, not places or property.[8] The Court has also found that the protection in s.8 is based on "reasonable expectations of privacy"[9], and that everyone has a reasonable expectation of privacy in their "biographical core of information"- i.e., information which tends to reveal intimate details of the lifestyle and personal choices of the individual.[10] Because CNA information (e.g., IP addresses and associated subscriber names) can easily be linked with online activities and communications that expose intimate details of an individual's life, it engages reasonable expectations of privacy, and thus section 8 of the *Charter*.

28. In order for a search to be considered "reasonable" under section 8, courts have found that there must be "reasonable and probable grounds" to suspect that a crime has been committed.[11] Practically speaking, and most often, this means that a search and seizure must be judicially authorized, after the judge has been satisfied that there are reasonable and probable grounds to believe criminal activity has taken place or will take place.[12]

29. Exceptions to this fundamental rule of due process may be permitted under section 1 of the *Charter* if they "can be demonstrably justified in a free and democratic society." The Supreme Court has set out the following test to determine whether a given measure can be so justified:
    - There must be a *pressing and substantial objective*; and
    - The means must be *proportional*; which implies that:
        (i) the means must be *rationally connected* to the objective;
        (ii) there must be *minimal impairment* of rights; and
        (iii) there must be proportionality between the infringement and objective.[13]

30. We question whether the proposal for warrantless access to CNA information would pass *Charter* scrutiny, given the less invasive law reforms that could be implemented to address

---

[6] *Ibid*.
[7] Section 1 of the *Charter,* however, allows for "such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society."
[8] *Hunter v. Southam Inc*., [1984] 2 S.C.R. 145, at para 23, Dickson citing *Katz v.United States*, 389 U.S. 347 (1967).
[9] *Ibid.* at para 24.
[10] *R. v. Plant* [1993] 3 S.C.R. 281 at 293.
[11] *Supra* note 2 at para 43.
[12] *Supra* note 2 at para 28-29.
[13] *R. v. Oakes*, [1986] 1 S.C.R. 103, 24 C.C.C. (3d) 321, 50 C.R. (3d) 1 at paras 69-71.

the problems raised by law enforcement agencies (see above), and the disproportionate impact on individual privacy that warrantless access to CNA information would have, especially in light of the weak oversight and accountability mechanisms currently in place for law enforcement agencies in Canada.

31. Moreover, the internet is a vibrant forum for expression of political dissent and unpopular views, as well as for the sharing of highly personal information, in large part because of the anonymity that it offers to people. In this context, individuals should not be stripped of their anonymity without due process. Otherwise, valuable free speech (as protected by section 2 of the *Charter*) will be chilled.

32. CIPPIC submits that Canadians have a reasonable expectation of privacy in their CNA information, that forced access to that information constitutes a search and seizure, and that such a search therefore requires prior authorization based on reasonable grounds to suspect criminal activity. Allowing for such searches without warrants or other judicial authorization on a "reasonable grounds" basis would, in our submission, violate the *Charter*.

Safeguards

33. The primary safeguard against police abuse of investigative powers is the requirement for prior judicial authorization before a search or other surveillance activity takes place, based on a "reasonable grounds" standard. The proposal in question would do away with precisely that safeguard. For this reason, we object to it.

34. Another critical safeguard is the existence of effective oversight mechanisms to guard against and punish abuse of power. As the Arar Commission's report makes clear, current oversight mechanisms for Canadian national security and law enforcement agencies have proven themselves inadequate in preventing inappropriate sharing of personal information among law enforcement agencies.[14] Without improvements to our current oversight mechanisms, we should not be granting any additional powers to law enforcement agencies.

35. In this respect, we support the Ontario Information and Privacy Commissioner's call for the creation of an independent oversight body to supervise lawful access activities of law enforcement agencies and ensure public accountability, transparency, and scrutiny, and to enhance public confidence, especially if any new "lawful access" powers are granted to law enforcement agencies.[15]

36. The Consultation Paper proposes a number of "possible safeguards", some of which are aimed at oversight. These include:

---

[14] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (Ottawa: Public Safety and Emergency Preparedness Canada, 2006). Online: <http://www.ararcommission.ca/eng/AR_English.pdf>

[15] The Ontario Information and Privacy Commissioner proposed such a body in its submission to the Minister of Justice and Attorney General of Canada on the 2005 "Lawful Access" Consultations. See <http://www.ipc.on.ca/index.asp?layid=86&fid1=105>

- 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.

37. In our submission, internal auditing requirements and discretionary external audits by the Privacy Commissioner of Canada and SIRC are insufficient. Agencies have a strong disincentive to revealing their own errors and weaknesses. Moreover, existing oversight bodies often lack the resources to take on new tasks that they are not mandated to take on. For these reasons, effective oversight should include:
    - a mandatory external audit;
    - mandatory reporting to the Minister and oversight agencies; and
    - a mechanism for public accountability (e.g., reporting to Parliament; publishing of reports).

38. The Consultation Paper suggests a number of other possible safeguards, including:
    - 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.

39. In order for auditing and accountability mechanisms to be effective, officers accessing CNA information should be required to keep detailed records including the purpose for demanding access – not just "the duty or function for which a particular request is made".

40. With respect to safeguards against misuse of information gathered, we submit that there should be strict limits on disclosure as well as use of the information gathered. Moreover, there should be stiff penalties for opportunistic use, or misuse of information accessed through the new power.

41. Even with all these safeguards, however, the proposal to permit warrantless access to CNA information remains in our view fundamentally flawed due to its over-broad nature – i.e., permitting access without warrant or reasonable grounds as long as it is "for the purpose of

performing an official duty or function". If law enforcement agencies are to be granted wider powers to access this information, a key safeguard is to limit the purposes for which they can demand access much more narrowly than this.

Conclusion

42. Information identifying telecommunications subscribers can be highly sensitive given the electronic trail of publicly available and otherwise accessible data that individuals now leave about themselves on the internet and other digital devices as they go about their daily lives. For this reason, we submit that CNA information raises a "reasonable expectation of privacy" on which a *Charter* challenge to laws permitting warrantless access could be based.

43. Moreover, we remain skeptical about the need for these potentially intrusive and far-reaching measures. It is not clear that greater access by law enforcement to electronic communications will, in fact, increase the security of Canadians; and it has not been demonstrated that no other, less privacy-intrusive, measure would suffice to achieve the same purpose of enhanced security. In particular, the permitted purposes for demanding CNA information are far broader than required to solve specific problems such as gaining access to next-of-kin information in emergency situations, or acting on tips quickly in exigent circumstances.

44. Finally, the safeguards proposed are insufficient, in our view, to protect individuals from over-reaching and abusive exercise of police powers. In particular, there should be no expansion of police investigatory powers without a corresponding increase in independent oversight.

Sincerely,

Philippa Lawson
Director, CIPPIC

Jocelyn Cleary
Student-at-law, CIPPIC