OFFICE OF THE PRESIDENT
CABINET DU PRÉSIDENT

October 18, 2007

Lynda Clairmont
Associate Assistant Deputy Minister
Emergency Management and National Security Branch
Public Safety Canada
269 Laurier Avenue West
Ottawa, ON K1A 0P8

Dear Ms. Clairmont:

Re: Customer Name and Address Information Consultation

I write in response to your letter dated September 11, 2007, seeking our comments on Public Safety Canada's Customer Name and Address (CNA) Information Consultation Document. This letter summarizes the Canadian Bar Association's (CBA) concerns about proposals pertaining to law enforcement and national security agencies' access to CNA information held by telecommunications service providers (TSPs). Thank you for the opportunity to contribute our views on this important subject.

The CBA is a national professional organization representing over 37,000 lawyers, notaries, law students and teachers from every part of Canada. The CBA's mandate includes seeking improvements in the law and the administration of justice.

Fundamental Principles

In previous consultations on what have been referred to as "lawful access" proposals in 2002 and 2005, the CBA emphasized several fundamental principles. We stressed that all initiatives must be constitutionally valid and reflect fundamental values of Canada's *Charter of Rights and Freedoms*. As a prerequisite to any new investigative powers, we noted that the need for those new powers must be clearly demonstrated and that the measures proposed be carefully tailored to provide the maximum respect for individual rights. We have previously articulated the fundamental importance of the balancing process required as follows:

500 - 865 Carling, Ottawa, Ontario Canada K1S 5S8
Tel/Tél. : (613) 237-2925 Toll free/Sans frais : 1-800-267-8860 Fax/Télécop. : (613) 237-0185
Home Page/Page d'accueil : www.cba.org E-Mail/Courriel : info@cba.org

> *Living in a democracy requires that the state should not interfere with, or restrict the rights, liberty or security of individuals without a demonstrated need. Where there is compelling evidence of such a need, the law or other action of the state should be tailored so that the restriction on, or interference with individual rights is no greater than absolutely necessary to accomplish the objective of the law or state action.*[1]

We repeat that the twin principles of demonstrated necessity and minimal intrusion must form the foundation of any proposals to advance or extend search and seizure powers. This foundation also provides the essential context in which the constitutional validity and efficacy of new measures must be assessed.

The CBA has also previously expressed strong concerns about the potential of various lawful access proposals to profoundly impact the privacy of individual Canadians. We have particularly noted, amongst our other concerns, the potential to destroy solicitor client privilege by violating communications between lawyers and clients.[2]

While we appreciate that access to CNA information has been the subject of previous consultation, the rapid evolution of technology and investigative practice requires careful consideration of the context in which these current proposals are made. In our view, the present context is not described in sufficient detail to permit definitive conclusions about these proposals. However, we believe that this consultation provides an opportunity to articulate a principled framework in which these issues can properly be considered.

Explicit Legal Authority

As noted in the consultation document, a wide variety of practices have developed regarding the release of CNA information to law enforcement authorities. The CBA welcomes recognition of the need for explicit legal authority for the mandatory release of this personal information.

The inconsistent practices of Canadian organizations in general and TSPs in particular, as mentioned in the consultation document, are a direct result of the challenges many organizations have in applying the *Personal Information and Electronic Documents Act* (PIPEDA), specifically section 7(3). PIPEDA provides a regime that governs the collection, use and disclosure of personal information by the private sector, generally requiring knowledge and consent of the individual to whom the personal information pertains. However, section 7(3) also provides for specific limited circumstances where personal information may be collected, used and disclosed without an individual's consent. Relevant to this consultation are section 7(3)(c) regarding warrants and court orders, section 7(3)(c.1) where a request is made by a government institution that has identified its lawful authority, and section 7(3)(i) where the disclosure is "required by law".

The circumstances when a warrant or court order is presented or when disclosure is required by law elicit little confusion. However, there has been significant uncertainty and confusion as to exactly what "lawful authority" includes in relation to requests from law enforcement agencies (LEAs). A detailed analysis of "lawful authority" as intended in section 7(3)(c.1) is beyond the

---

1 Canadian Bar Association, *Submission on Lawful Access* (Ottawa: CBA, 2005) at 1.

2 Canadian Bar Association, Letter from then CBA President B. Tabor to then Ministers of Justice, Public Safety and Industry (Ottawa: CBA, 5 July 2006).

parameters of this consultation. However, it is relevant to note that some LEAs point to this section of PIPEDA as actually constituting their "lawful authority" to obtain the requested information. Certain LEAs have even formulated a "letter of authority" to request CNA information, referring to PIPEDA as their lawful authority.

In fact, section 7(3)(c.1) cannot constitute lawful authority to obtain the requested information. Rather PIPEDA establishes a discretionary regime pursuant to which organizations ***may*** disclose personal information when the relevant requirements of the section in question have been met.

The effect of the amendments proposed in the consultation document would be to remove uncertainty for certain private sector organizations (i.e. TSPs) as to any discretion to disclose the CNA information specified in the consultation document: according to the proposals, they would be "required by law" to disclose the specified information. However, while the consultation document clarifies the nature of an order that would give rise to an obligation to disclose, we note that private sector organizations would continue to have discretionary ability to disclose certain information pursuant to applicable privacy legislation such as PIPEDA.

Prior Judicial Authorization and Reasonable Expectations of Privacy

The consultation document proposes an administrative scheme where a designated officer could demand disclosure of CNA information. Several possible safeguards are suggested in the consultation document, many that appear to respond to some of the issues raised in earlier consultations.[3] We have two principal concerns regarding the model proposed in the consultation document.

First, the disclosure of the stipulated information upon demand appears to be at least partly based on the idea that PIPEDA would not restrict disclosure of certain material because it is already in the public domain through sources such as telephone directories. In fact, PIPEDA does not distinguish between sensitive and non-sensitive information in this context. PIPEDA does permit the disclosure of personal information that is both publicly available ***and*** specified by the regulations. However, most of the information listed in the consultation document is not actually publicly available and is also not specified by the regulations. Still, as noted, disclosures in such contexts fall under a discretionary responsibility and the other PIPEDA provisions would continue to apply to any discretionary disclosure.

Second, the scope of the information listed in the consultation document is much too broad, and extends beyond what might be appropriately regarded as "basic information". Responses to previous consultations on this topic also expressed concern about the scope of proposed lists.[4]

Concerns about the scope and nature of such information must be measured against the constitutional concept of a reasonable expectation of privacy. This concept defines the threshold at which prior judicial authorization for a search will be required.[5] However, it is sometimes difficult to determine precisely where that threshold will fall. The Supreme Court of Canada has

---

3 See for example the response of the Federal Privacy Commissioner to a similar proposal in 2005, "Response to the Government of Canada's "Lawful Access Consultations", available online at http://www.privcom.gc.ca/information/pub/sub_la_050505_e.asp

4 *Ibid.*

5 See for example, *Canada* v. *Southam Inc.*, [1984] 2 S.C.R. 145.

noted that the determination of where a reasonable expectation of privacy will be found is a contextual exercise, requiring a careful balance between the rights of the individual and the legitimate interests of society in effective law enforcement.[6] As technology and investigative practices evolve, previously constitutional activities conducted without warrant may require a warrant. The extent to which changes in technology and practice enable the discovery of "core biographical information" or reveal "intimate details regarding lifestyle" may necessitate prior judicial authorization.[7] Further, the current technological capability to combine various sources of information to reveal additional details about individuals is a significant factor that may favour prior judicial authorization.[8] The CBA believes that a continuing review of any administrative model would be imperative to ensure that changes in technology and practice do not result in a process that violates the *Charter*.[9]

Administratively authorized search procedures, as opposed to court ordered procedures, have been particularly susceptible to abuse. In the United States, a recent review of "National Security Letters" issued pursuant to the *Patriot Act* revealed significant irregularities and abuse in the program.[10] The Office of the Inspector General documented that the use of National Security Letters increased exponentially after that power was expanded in the *Patriot Act*.[11] Difficulties and discrepancies in internal record keeping practices and controls complicated the task of compiling accurate statistics.[12] The American experience should serve as a warning for Canada in relation to administrative programs, and illustrates that significant problems can arise even when a program includes internal restrictions and safeguards.

On a practical note, careful consideration must be given to the impact of increased internal procedures and protocols on the ultimate speed and efficiency suggested as advantages of the administrative model. One result of the appropriate proliferation of internal protocols and safeguards may be to narrow any difference in the time involved between the administrative and judicial authorization process. If this gap is significantly narrowed, diminished practical benefits of the administrative approach must be assessed against the shortcomings and difficulties of that approach noted above. It is important to consider that internal safeguards cannot replicate certain benefits of prior judicial authorization, such as those associated with maintaining public confidence in our laws. Careful consideration must also be given to existing mechanisms contained in the *Criminal Code* that either enable searches for certain information at lower thresholds, or through the use of an expedited process.

---

6 *R. v. Tessling* 2004 S.C.C. 67 at paras. 17-18. See also *R. v. Plant,* [1993] 3 S.C.R. 281 at 293.

7 *Tessling*, *ibid.,* at paras. 59-62.

8 For example, the impact of new technology on the ability to combine such sources, together with the resulting loss of privacy is described in the context of "data mining" in Renee Pomerance, "*Redefining Privacy in the Face of New Technologies: Data Mining and the Threat to the "Inviolate Personality"* (2006) 9 Can. Crim. L. Rev. 273.

9 We appreciate that Public Safety Minister Stockwell Day has stressed that personal information requires the ongoing protection of judicial authorization.

10 *A Review of the Federal Bureau of Investigation's Use of National Security Letters",* March 2007, United States Department of Justice, Office of the Inspector General, Executive Summary at 34-50. Available online at http://www.usdoj.gov/oig/special/s0703b/final.pdf

11 *Ibid.,* at 17.

12 *Ibid.* at 17-19.

In our responses to the last two consultation documents on lawful access in 2002 and 2005 and elsewhere, the CBA suggested that a comprehensive approach to search and seizure powers in the *Criminal Code* is needed. Such an approach should encompass all forms of search and seizure in a dedicated part of the Code, including intercepts, CNA information, tracking warrants, general warrants and other types of search and seizure.

Finally, the consultation document suggests that information could be obtained for purposes of notification of next of kin or other similar circumstances. However, it would be a relatively uncomplicated matter to deal with such situations. For example, TSPs might notify individuals involved that the authorities have information to provide to them, or specific legislation could be passed to directed TSPs to provide CNA information in that context without prior judicial authorization. However, that unique context is significantly different than an investigation of a *Criminal Code* offence.

Role of the Police, CSIS and the Competition Bureau

The CBA is particularly concerned with the suggestion that the proposed powers should be granted concurrently to the police, CSIS and the Competition Bureau. The uses to which information may be put in the context of investigations by the Competition Bureau or CSIS differ significantly from that of LEAs under the *Criminal Code.*

In our submissions to the Air India Inquiry,[13] the CBA pointed out that information gathered for intelligence purposes is inherently different than information gathered for law enforcement purposes. Information for intelligence purposes is gathered without the expectation that it will ultimately be led as evidence in a court of law. The procedures for gathering, storing, recording and disclosing security information is completely different from that engaged in by police officers in respect to evidence under the *Criminal Code*. Generally, the actions of intelligence officers will never be subject to judicial review. Accordingly the requirement for prior judicial authorization is more, not less, pressing in the case of CSIS or any other agency involved in information gathering for intelligence purposes. As has unfortunately been seen in the Arar Inquiry,[14] intelligence information can be used to have devastating effect on a person's life, without any judicial intervention or review.

Likewise the nature of the *Competition Act* and the investigations conducted by the Competition Bureau under that Act are quite different from the type of investigation carried on by the police. In the context of the *Competition Act*, it is anticipated that voluminous documentation would be an inherent part of the process and that the breaches of law will be aimed primarily at unlawful financial advantage as opposed to threat of physical harm. Realistically, the Competition Bureau is unlikely to require CNA information on an urgent basis such that the absence of prior judicial authorization would be justified.

Conclusion

The CBA appreciates the opportunity to participate in ongoing consultations regarding lawful access and access to CNA information. We have stressed that the determination of constitutional norms in this regard is a context sensitive exercise. Any expansion of the search powers in the

---

13 Canadian Bar Association, *Submission to the Air India Inquiry* (Ottawa: CBA, 2007).

14 Canadian Bar Association, *Submission to the Arar Inquiry* (Ottawa: CBA, 2005).

Criminal Code or other legislation should not occur without a clear and demonstrable foundation. We welcome the opportunity to participate in further discussions once that context has been fully articulated, particularly in relation to present technical and practical capabilities.

We have noted several difficulties with an administrative search regime. The constitutional status of such a regime may be undermined by technological advances, changes in practice or the ability to combine or aggregate data from several sources. Further, there are inherent difficulties with an administrative approach such that it may be that in the long run a system based on prior judicial authorization provides the more constitutionally stable and effective approach. Finally, to the extent that the consultation document proposes a "one size fits all" approach for the *Criminal Code,* the *Competition Act*, and CSIS, we express our concern, and point to the very distinct roles of these statutes and agencies and the contexts in which they generally function. A proper approach must recognize those significant differences.

The issue of costs of complying with either a court order or an administrative order is a complex and contentious one. It is difficult to compare costs of an administrative scheme with one that relies on court orders, given factors such as indirect cost implications to the court system or direct cost implications to the law enforcement agency involved. The current proposals may also have cost implications for TSPs and other third parties. This has been the subject of other consultations, and is a complicated public policy issue. It is also the subject of continuing litigation.[15] We welcome the opportunity to comment during further consultations on this important related issue.

We note too that the issue of extraterritorial application of Canadian laws must be considered as the proposals in the consultation document may indirectly impact organizations or citizens from other jurisdictions. Again, this is a significant and complex issue in an increasingly globalized economy that involves, for example, many internet service providers and offshore data storage.

The CBA believes that the quality of any public consultation process is significantly enhanced by the level of detail provided in the consultation documents. To the extent possible it would be helpful to have concepts presented in as much detail as possible, including examples of draft language for the proposals in question.

We look forward to continuing dialogue on these important issues, and thank you again for the opportunity to participate in this consultation.

Yours very truly,

(original signed by Bernard Amyot)

Bernard Amyot

---

[15] See for example *R. v. Tele – Mobile*, tentatively scheduled to be argued in the Supreme Court of Canada in December of this year.