Submission on
Lawful Access - Consultation Document

CANADIAN BAR ASSOCIATION

December 2002

TABLE OF CONTENTS

Submission on
Lawful Access - Consultation Document

PREFACE

The Canadian Bar Association is a national association representing over 38,000 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice.

This submission was prepared by the National Competition Law, Media and Communications Law, and Criminal Justice Sections of the Canadian Bar Association, with assistance from the Legislation and Law Reform Directorate at the National Office. The submission has been reviewed by the Legislation and Law Reform Committee and approved by the Executive Officers as a public statement of the Canadian Bar Association.

Submission on *Lawful Access* - Consultation Document

I. INTRODUCTION

The Canadian Bar Association (CBA) is pleased to offer its comments regarding the *Lawful Access* Consultation Document released by the Department of Justice, Industry Canada and Solicitor General Canada on August 25, 2002 (Consultation Document).

Lawful access means the authority granted by legislation to provide "law enforcement and national security agencies with powers to intercept communications and search and seize information in a manner consistent with the rights and freedoms guaranteed in the *Canadian Charter of Rights and Freedoms*, particularly the right to be secure against unreasonable search and seizure."[1]

Our sense of what it is to live in a democracy requires that the state should not interfere with, or restrict the rights, liberty or security of an individual unless there is demonstrable need to do so. Further, where there is compelling evidence of such need, the law or other action of the state should be tailored such that the restriction on, or interference with individual rights is no greater than is necessary to accomplish the objective of the law or state action.

The CBA recognizes that effective policing and protection of national security are also essential considerations for our Canadian democracy. However, those considerations must not be too readily or zealously raised in support of intrusive measures by the state to the exclusion of, and as a substitute for, measured debate.

---

1 *Lawful Access* Consultation Document (Ottawa: Department of Justice, Industry Canada, Solicitor General Canada, 2002) at 3.

The need for effective policing and national security does not negate the need for careful and rational discussion of a proposed law. Rather, it is the very crux of the discussion. In other words, that a proposed law may be of benefit to law enforcement does not end the debate with respect to whether that proposed law is constitutional or otherwise desirable. Instead, it serves as the beginning of the discussion.

There are profound implications for privacy interests when the state collects data. Laws which permit intercepting and collecting information must accord with the principles, rights and values enshrined in the *Canadian Charter of Rights and Freedoms*.

When considering the broad range of proposals set out in the Consultation Document, we believe it is insufficient simply to measure each specific proposal against the *Charter* and to conclude that the proposal should become law on the basis that it may accord with the *Charter*. Privacy may be unduly eroded through the cumulative effect of state action and, for this reason, careful consideration must be given to the effect of the body of measures being proposed. This consideration must be made against the background of both other laws which undermine privacy, and the role and importance of personal privacy in Canadian democracy.

II. GENERAL PRIVACY CONSIDERATIONS

The following passages are relevant in considering the Consultation Document and demonstrate the Supreme Court of Canada's consistent recognition of the importance of zealously protecting privacy.

> If one is to give s. 8 the purposive meaning attributed to it by *Hunter v. Southam Inc*., one can scarcely imagine a state activity more dangerous to individual privacy than electronic surveillance. [2]

> ...the broad and general right to be secure from unreasonable search and seizure guaranteed by s. 8 is meant to keep pace with technological development, and, accordingly, to ensure that we are ever protected against unauthorized intrusions upon our privacy by the agents of the state, whatever technical form the means of invasion may take.[3]

> This court has adopted a liberal approach to the protection of privacy. This protection extends not only to our homes and intimately personal items, but to information which we choose...to keep confidential...As a 1972 task force on privacy and computers noted, informational privacy "derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain...as he sees fit."[4]

Consideration of the proposals in the Consultation Document must be informed by the Supreme Court of Canada's clear rejection of "risk analysis" as a basis upon which to assess the expectation of privacy.

> In *Duarte*, this court overturned the conclusion of the Court of Appeal that the risk that our interlocutor will electronically record our words is but a variant of the risk of having that person disclose our words to another. This court accordingly rejected the notion that "risk analysis" provides an appropriate means of assessing whether a person who was the object of an electronic search had a reasonable expectation of privacy in the circumstances. As explained at p. 14 of that decision, this rejection rested on the conclusion that privacy would be inadequately protected if an assessment of the reasonableness of a given expectation of privacy were made to rest on a consideration whether the person concerned had courted the risk of electronic surveillance. In view of the advanced state of surveillance technology, this would be to adopt a meaningless standard, for, in the final analysis, the technical resources which agents of the state have at their disposal ensure that we now run the risk of having our words recorded virtually every time we speak to another human being. [5]

Rather than by risk analysis, LaForest J. held that the problem of defining what constitutes a reasonable expectation of privacy in given circumstances is to be

---

2 *R. v. Duarte* (1990), 53 C.C.C. (3d) 1 at 10 (S.C.C.).

3 *R. v. Wong* (1990), 60 C.C.C. (3d) 460 at 477 (S.C.C.).

4 *R. v. Law* (2002), 160 C.C.C. (3d) 449 at 458 (S.C.C.).

5 *Wong*, *supra*, note 3 at 477.

approached "by the standards of privacy that persons can expect to enjoy in a free and democratic society."[6] In our view, this is the proper approach to privacy.

The lawful interception and collection of data, including private communications, is important to law enforcement in the simple and obvious sense that the powers of law enforcement will often be enhanced through access to information. It may be appropriate for existing laws to be amended to specifically refer to new technologies. However, while this consideration is relevant to the issue of law reform, it should not determine the direction or manner in which the law should evolve.

A. Privacy and E-mail

The use of e-mail as a means of communication is now common-place. The ease with which enormous amounts of data can be quickly transmitted makes e-mail highly efficient in terms of time and cost and, for this reason, widely used by both individuals and organizations.

The fact that e-mail necessarily requires that data which constitutes the communication be transmitted and, in some instances stored in a certain manner, does not in and of itself reduce the reasonable expectation of privacy users associate with e-mail communication or data. It is incorrect to conclude that users of e-mail court the risk of interception simply because the communication data is channeled in certain ways. It would be equally incorrect to conclude that the privacy associated with the communication is in any way diminished as a result of the channeling of the data which constitutes the communication.

The Consultation Document asks whether e-mail traffic is a "private communication" and whether it should be subject to a different type of order, that

---

6 *Ibid*., at 478.

is a wiretap authorization versus a search warrant, depending on the stage of communications at which it is intercepted.

Many e-mail communications are sent in confidence, or with content expressly designated as such. Many are deleted by the recipient upon reading – precisely because it is considered inappropriate or unnecessary to keep a record of such communication. All, or virtually all, are sent with the expectation that the state will not be receiving copies. The CBA believes that interception of e-mail traffic constitutes interception of a "private communication". As such, it should be subject to the same requirements for a judicial authorization as for a wiretap. It is difficult to find a principled distinction between keyboarding, transmission between a sender's computer and the sender's Internet Service Provider (ISP), transmission between the sender's ISP and the recipient's ISP, or transmission between the recipient's ISP and the recipient's computer. This is simply the technological routing associated with this form of private communication. There is an argument that once communication data is stored, it can be seized in a manner similar to seizing an envelope, and therefore that the data does not deserve the full protection of a Part VI authorization. However, this argument fails to recognize that the communication is by its very nature private, and therefore indistinguishable from a telephone conversation. E-mail is a form of private communication, and interception at any point should be subject to the protections contained in a Part VI authorization.

If service providers are to be *compelled* to now share subscriber information, and also *compelled* to have the technical capability of intercepting communications, we suggest that there must be wide and general notification to the public of these requirements.

Finally, making it an offence to *receive* forbidden communications is more than troublesome, given the quantity of unsolicited e-mail transmitted every day to unwilling recipients. This should be an offence only if the communication has

been requested, with knowledge of the kind of content it will bear. People who receive obscene phone calls are not themselves guilty just by receiving them.

III. PROCESS CONCERNS

The Consultation Document raises many issues for debate, but is insufficiently precise to form an adequate basis for meaningful consultation. Further consultation, including an opportunity to comment on the specific proposals contained in draft legislation is called for. While the CBA is very pleased to have the opportunity to provide comments on some of the general themes and proposals in the document, without specific legislative proposals, our remarks are necessarily somewhat tentative.

Few would argue with the basic premise that law enforcement personnel need investigative tools that take account of modern technology. If judges authorize police to monitor private communications, the lack of technological expertise should not be such as to frustrate that authorization.

The Consultation Document lacks specific suggestions for achieving an appropriate balance between public and private interests. For example, we are aware of certain proposals being considered by concerned government departments and agencies, but the details of such proposals are not found in the Consultation Document. At page 6, we read that "the proposals in this document are points of departure for discussion." Again, a meaningful discussion of the issues raised will require further consultation on specific proposals and on draft legislation and regulations, prior to introduction in Parliament.

For example, with respect to the relative burdens of providing technology for law enforcers to intercept telecommunications transmissions, the details will apparently be contained in regulations – drafts of which the Consultation

Document does not commit to exposing to public comment prior to adoption of any particular model. Essentially, industry is being told that the issues have been studied extensively and options are being considered; this is insufficient.

Similarly, with respect to important compliance mechanisms, we wonder which alternatives are being considered. On page 12, it states that "a specific production order to be issued under a lower standard could also be created to obtain other data or information in relation to which there is a lower expectation of privacy." What "other data or information" does the government have in mind?

The lack of depth of the consultation process is perhaps exemplified by the statement at page 17 under "Other Orders". It says merely that "this proposal involves the ability to obtain general warrants and assistance orders to enhance the efficacy of evidence gathering tools." We wonder, "What proposal?", "How are existing tools inadequate?", "How will general warrants and assistance orders assist?", "What precise powers would be granted, and what would be the judicial test for their authorization?" and "What alternatives were considered and why were they rejected?". As things stand, the Document is essentially a "trust us" document.

A. Omitted Proposal

The dearth of detail is all the more apparent when we consider that the Consultation Document contains no mention of an important proposal which we have been told by government officials is under consideration. The proposal is to appoint employees of the Competition Bureau as peace officers to deal with potentially volatile situations they encounter in executing search warrants at the premises of suspected criminal telemarketers and in connection with legal proceedings against them. Apparently, having members of the RCMP Commercial Crime Unit accompany Bureau officers on such "raids" would be considered optimal, as the mere presence of RCMP officers has a salutary effect on the behaviour of those under investigation or prosecution. But coordination

with that unit is difficult. If this is indeed a proposal being considered, we believe that expecting commerce officers and economists to be transformed into peace officers merely by designating them as such would be dangerous for all concerned. Clearly, what is needed would be better coordination with the RCMP, so that personnel with the training and experience to defuse potentially volatile situations, or deal with intimidation tactics, are available to the Bureau on a timely basis. For example, arrangements could be made for designation of RCMP personnel specifically responsible for assisting in *Competition Act* matters, and if demand warranted, an officer could be assigned to the Bureau.

IV. CONSISTENCY IN DEFINITION

The Consultation Paper provides working definitions for various telecommunications terms as part of its proposal. Of critical importance is the following definition of "service provider":

> "Service provider" is defined as a person who owns or operates a transmission facility that is used by that person or another person to provide telecommunications services to the public in Canada.[7]

The definition does not draw the distinction between *ownership* and *operation* of transmission facilities, on the one hand, and mere *use* of those facilities, on the other. This distinction is crucial for regulation purposes under the *Telecommunications Act.* The C.R.T.C. has determined[8] that only those entities that both own *and* operate transmission facilities qualify as "telecommunications common carriers" under the *Telecommunications Act* and are subject to regulation by the C.R.T.C. as such, while entities that merely *operate* such facilities (*e.g.*, resellers) are subject to significantly reduced regulatory oversight. This finding was made to reflect the legislative intention of Parliament to exclude "resellers"

---

7 *Supra*, note 1 at 4.

8 *Exemption of Resellers from Regulation*, Telecom Public Notice C.R.T.C. 93-62, October 4, 1993.

from the obligations imposed on telecommunications common carriers under the *Telecommunications Act*.

It is also unclear whether only service providers are "telecommunications common carriers" (within the meaning ascribed by the C.R.T.C.) intended to be subject to any new laws relating to lawful access, or whether all service providers, including resellers, would be subject to such laws.

"Telecommunications facility" is not defined in the Consultation Document, although s. 2(1) of the *Telecommunications Act* contains a definition. The Consultation Document contains a working definition of a "transmission facility" (at page 7) which is similar, but not identical, to the definition of a "transmission facility" contained in the *Telecommunications Act*:

> "Transmission facility" means any wire, cable, radio, optical or other electromagnetic system, or any other (similar) technical system, used for the transmission of information between network termination points.

It is difficult to see a valid justification for slightly amending definitions that are already established in, and familiar to industry. By introducing even minor variations, we run the risk of generating unnecessary confusion.

V. JURISDICTION

The Consultation Document does not address the basis for the federal government's constitutional jurisdiction to impose the lawful access requirement on all three types of "service providers" identified in the Consultation Document (i.e., wireless, wireline and Internet). The working definitions in the Consultation Document do not assist in addressing the jurisdictional issue raised by ISPs and other entities that are not telecommunications common carriers. The Consultation Document proposes that all "service providers (wireless, wireline and Internet) have the technical capability to provide lawful access to law enforcement and national security agencies"(at page 7). At page 8, the

description of the entities subject to the lawful access requirement is refined, stating that the "legislation would apply to all service providers operating a telecommunications facility in Canada." As noted above, "telecommunications facility" is not defined in the Consultation Document.

The federal government's power to legislate in relation to the criminal law under s. 92(27) of the *Constitution Act, 1867*, may well provide the basis upon which to impose lawful access requirements upon service providers. However, the Consultation Document is silent in this regard.

The lawful access proposal could also apply to a "service provider" under federal legislative competence as an inter-provincial undertaking, pursuant to s. 92(10)(a) of the *Constitution Act, 1867*.[9] *Alberta Government Telephones (AGT) v. Canadian Radio-television and Telecommunications Commission* [10] is the leading case on whether an undertaking providing telecommunications services constitutes an inter-provincial undertaking falling within federal jurisdiction. The Supreme Court of Canada followed the analysis from *Construction Montcalm Inc.* v. *Minimum Wage Commission*[11] and stated:

> There is ample authority for the proposition that the crucial issue in any particular case is the nature or character of the undertaking that is in fact being carried on. … It is impossible, in my view, to formulate in the abstract a single comprehensive test which will be useful in all of the cases involving s. 92(10)(a). The common theme in the cases is simply that the court must be guided by the particular facts in each situation, an approach mandated by this Court's decision in *Northern Telecom, 1980, supra.*[12]

9 30 & 31 Victoria, c. 3.

10 [1989] 2 S.C.R. 225 [hereinafter the *AGT* case].

11 [1979] 1 S.C.R. 754.

12 *Ibid*.

The Court concluded that *AGT* was an inter-provincial undertaking,[13] establishing that telecommunications common carriers (i.e. those entities that own or operate the facilities, including wires, cables, radio, optical and electromagnetic spectrum) used to provide telecommunications services to customers in Canada are inter-provincial undertakings subject to federal jurisdiction under s. 92(10)(a) of the *Constitution Act, 1867*. In *Capital Cities Communications v. C.R.T.C.,*[14] the Supreme Court held that s. 92(10)(a) was the basis of federal jurisdiction over broadcast television. Professor Peter Hogg has argued that it is probably safe to assume that federal jurisdiction over radio communication is also based on s. 92(10)(a).[15]

However, these cases do not answer whether service providers, such as ISPs, that are both not carriers and do not own or operate transmission facilities, will also constitute inter-provincial works or undertakings. The careful, fact-specific review suggested by the case law is absent from the Consultation Document in respect of ISPs.

It is also unclear whether "non-carriers" would necessarily fall within the ambit of the proposed working definitions for "service provider" or "transmission facility" contained in the Consultation Document. For example, many ISPs neither own nor operate "transmission facilities" as defined in the working definition. Often, ISPs lease such facilities from other carriers, and so would fall outside the working definition of "service provider". In any event, the Consultation Document contains no analysis of various types of ISP services, network and operational configurations and agreements to demonstrate that an ISP that neither owns nor operates transmission facilities would constitute an inter-provincial undertaking subject to federal jurisdiction.

---

13 *Ibid.*, 260-268.

14 [1978] 2 S.C.R. 141.

15 Peter Hogg, *Constitutional Law of Canada*, Looseleaf Ed., vol. 1 (Toronto: Carswell) at 22-26 [hereinafter, Hogg].

The federal government's residual peace, order and good government power (POGG) may provide an alternative basis for federal jurisdiction to impose lawful access capabilities over ISPs.[16] The jurisprudence interpreting POGG has identified three bases on which federal jurisdiction may be exercised:

- to fill lacunae or gaps in the distribution of powers scheme;
- to address matters of national concern; and
- to deal with national emergencies, which the courts have held are by definition temporary, which is obviously not the case here.

The gap doctrine holds that POGG power allows the federal government to exercise power where the *Constitution Act* has failed to expressly assign jurisdiction for a particular matter. Professor Hogg has suggested that recent Supreme Court of Canada jurisprudence shows a renewed acceptance of the reasoning in the *Radio Reference ,*[17] which held that POGG provides the federal government power to enact and implement treaties entered into by Canada on its own behalf because this power was not expressly provided for in the *Constitution Act*. [18] If so, it could be argued that Canada's status as a signatory to the Council of Europe *Convention on Cyber-Crime* and the need for Canada to enact legislative changes to the *Criminal Code* to ratify the treaty, all of which is alluded to at pages 5 and 6 of the Consultation Document, arguably serve as a basis for federal jurisdiction.

Alternatively, POGG power can be founded in the national concern doctrine, which holds that matters which may once have been purely local or provincial in scope can take on an importance making them matters of national concern.[19] If federal jurisdiction is to be found on the basis of threats to national security or a

16 The relevant constitutional provision is the introductory portion of s. 91 of the *Constitution Act, 1867*.

17 *Re Regulation and Control of Radio Communication in Canada,* [1932] A.C. 304.

18 *Hogg, supra*, note 16.

19 *Ibid.*, at 403.

perceived emergency, the Consultation Document again omits any meaningful analysis supporting federal jurisdiction over service providers on that basis.

Given these considerations and in the interest of transparency, we recommend that the federal government explicitly clarify its analysis for assuming jurisdiction to subject non-carrier ISPs to the lawful access requirements.

VI. OTHER ISSUES FOR CONSIDERATION

A. Telecommunications Policy

S. 7 of the *Telecommunications Act* sets out the objectives of Canadian telecommunications policy pursuant to s. 47 of the *Act*. C.R.T.C. must exercise its powers in accordance with the Canadian telecommunications policy objectives. S. 7 recognizes that telecommunications plays an essential role in maintaining Canada's identity and sovereignty. Four of the objectives are important in this context:

- to render reliable and affordable telecommunications services of high quality accessible to Canadians in both urban and rural areas in all regions of Canada;
- to enhance the efficiency and competitiveness, at the national and international levels, of Canadian telecommunications;
- to foster increased reliance on market forces for the provision of telecommunications services and to ensure that regulation, where required, is efficient and effective; and
- to contribute to the protection of the privacy of persons.

Contrary to these objectives, the Consultation Document proposals could impose financial burdens on telecommunications carriers and other service providers that make it difficult for them to compete at national and international levels. In addition to ensuring that all significant upgrades of their equipment comply with

the new law, service providers will have to meet the search and seizure demands of national and foreign investigative authorities. Businesses that do not comply will receive sanctions and may be held criminally responsible if they fail to supervise users that participate in potentially illegal acts. The result is a legitimate concern that the proposals may ultimately result in market exit by both fledgling and established service providers.

i. Costs of Ensuring Intercept Capabilities

Implementation of the lawful access measures in relation to intercept capabilities contemplated in the Consultation Document could entail considerable costs for industry. Although it speaks of a "cost allocation regime" which would cover three main sets of circumstances, the Consultation Document fails to describe any of the allocation regime(s) that would apply in these circumstances. In fact, the Consultation Document avoids the allocation issue and simply presumes that service providers will bear the costs of upgrading of their systems.

ii. Forbearance

Because compliance with any new lawful access rules may not be feasible in all circumstances, the Consultation Document contemplates the possibility of creating a forbearance mechanism to remove the obligation of complying with the new rules for a specified time. The Consultation Document does not elaborate, except to mention that Cabinet may delegate the authority to forbear jointly to the Solicitor General and the Minister of Industry, and that administrative guidelines would have to be prepared. There is also no indication of the circumstances under which a forbearance order may be justified or of the criteria that will be used to evaluate when, and for how long, such orders will be valid. Any rules or standards in relation to the forbearance power must be clear, transparent and adhere to the principles of administrative law and natural justice.

B. Production Orders

Subject to one exception, nothing in principle should stand in the way of a production order, properly authorized, from being incorporated into the *Criminal Code*. What constitutes proper authorization will depend on the subject matter of the proposed seizure and the privacy interest attaching to that subject matter.

The exception is that a production order should not be available to compel those accused, suspected, or targeted by an investigation to participate in the investigation against themselves through the production of information. Such an order would very likely contravene *Charter* guarantees against self incrimination.

C. Virus Dissemination

The CBA is not opposed in principle to the creation of a new offence in relation to virus dissemination. However, we will need to consider the specific wording of any new offence being contemplated before providing support for such an addition.

VII. CONCLUSION

Simultaneous to the modernization of Canada's criminal law enforcement regime and the expansion of lawful access capabilities, the government, law enforcement agencies and the courts must seriously take into account the rights of Canadians to privacy and protection from unreasonable interference with such privacy. The expansion of lawful access requires very careful oversight.

We believe that a narrow, formalistic, or legalistic approach to assessing the issues raised by Consultation Document is inappropriate. We must instead consider these issues by reflecting upon fundamental notions, including the importance of privacy as it relates to the individual, the importance of privacy within and as a component

of Canadian democracy, the competing interests of data collection privacy, and law enforcement and national security within existing world conditions.

In regard to the proposals in the Consultation Document, we have made a number of recommendations, including that:

- careful consideration be given to the cumulative effect on the protection of privacy of all existing and new legislative proposals dealing with lawful access;
- that interception of e-mail traffic be considered interception of a "private communication" and therefore subject to the protections contained in a Part VI authorization;
- that if service providers are to be compelled to share subscriber information and have the technical capability of intercepting communications, there should be general public notification of this requirement;
- that careful consideration be given before making it an offence to receive forbidden communications, given the amount of unsolicited e-mail transmitted every day to unwilling recipients;
- that opportunities be provided for further consultation on lawful access, including an opportunity for the CBA to comment on the specific proposals contained in draft legislation;
- that the federal government explicitly clarify its analysis for assuming jurisdiction to subject non-carrier ISPs to the lawful access requirements;
- that any rules or standards in relation to the forbearance power be clear, transparent and adhere to the principles of administrative law and natural justice, and
- that any production orders introduced should not be available to compel those accused, suspected, or targeted by an investigation to participate in the investigation against themselves through the production of information.