Comments on the Government of Canada's *Lawful Access Consultation Document*

Submission to
Department of Justice
Industry Canada
Solicitor General Canada

BC Freedom of Information and Privacy Association
December 16, 2002

Acknowledgements

FIPA would like to thank Barbara Norell, LLB
of the law firm of Harper Grey Easton for her work
in preparing this submission

We wish to gratefully acknowledge the Law Foundation of British Columbia
for their ongoing support of FIPA's activities in the areas of law reform, research and
public education

THE LAW FOUNDATION OF BRITISH COLUMBIA

BC Freedom of Information and Privacy Association
103 - 1093 West Broadway, Vancouver, BC V6H 1E2
Ph: 604-739-9788 • Fax: 604-739-9148 • Email: info@fipa.bc.ca • Web: www.fipa.bc.ca

FIPA Comments on
the Government of Canada's
Lawful Access Consultation Document

Table of Contents

FIPA

BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION

December 16, 2002

Lawful Access Consultation
Criminal Policy Section
5th Floor, 284 Wellington Street
Ottawa, ON K1A 0H8

Dear Sirs/Mesdames:

COMMENTS ON THE *LAWFUL ACCESS CONSULTATION DOCUMENT*

The B.C. Freedom of Information and Privacy Association ("FIPA") welcomes the opportunity to comment on the federal government proposals as set out in the *Lawful Access Consultation Document* ("Consultation Document").

FIPA is an organization devoted to the protection of Canadians' rights of privacy and access to information. Our objectives include defending the right to personal privacy enjoyed by the citizens of Canada. We also recognize the need of law enforcement and national security agencies to be able to work effectively to ensure a safe and secure society.

Please note that this submission has been prepared with input from, and has been endorsed by, a number of organizations who were unable to prepare their own submissions, but who wished to present their views to the federal government. These groups are listed at the end of this submission. FIPA sponsored two Vancouver workshops on the Lawful Access proposals – the first at the request of the Department of Justice and the second in collaboration with Simon Fraser University's School of Communication – and received the input of over 45 groups and individuals.

In the context of telecommunications, Lawful Access is the interception of communications and the search and seizure of information carried out pursuant to legal authority as provided in Canadian law. The federal government proposes legislative amendments which are said, in part, to be required to ratify the Council of Europe *Convention on Cyber-Crime* ("Convention"), and to provide law enforcement agencies with the technical and legal capability to maintain lawful access when new technologies are used in connection with criminal activity.

We are opposed to the proposals in the Consultation Document, as they unjustifiably intrude upon the privacy rights of Canadian citizens.

THE RIGHT TO PRIVACY

In analyzing proposals for access to information that intrude upon citizens' rights to privacy, one must start with Constitutional principles set out in the *Charter of Rights and Freedoms* ("*The Charter*"). *The Charter* guarantees citizens the right to be secure against unreasonable search or seizure, subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.

The right to privacy has long been recognized as one of the interests protected by s.8 of the Charter. In *Hunter v. Southam Inc.* [1984] 2 S.C.R. 145, the court held the purpose of s. 8 includes the protection of individuals' reasonable expectation of privacy. It limits government action that infringes on that right. In assessing those limits, the right of individuals to privacy must be balanced against the interest of government in law enforcement.

The right to privacy is important to our personal autonomy and the foundation of our democratic nation. As stated *R. v. Dyment* [1998] (S.C.C.),

> Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for the public order. The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state.

In assessing proposals for electronic surveillance (such as are proposed in the Consultation Document), one must be mindful of the discussion of the majority of the court in *R. v. Duarte* [1990] 1 S.C.R. 30:

> "I begin by stating what seems to me to be obvious: that, as a general proposition, surreptitious electronic surveillance of the individual by an agency of the state constitutes an unreasonable search or seizure under s.8 of the Charter.
>
> …
>
> 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 and to which, in consequence, the protection accorded by s.8 should be more directly aimed.
>
> …
>
> The reason for this protection [regulating the power of the state to record communications] is the realization that if the state were free, at its sole discretion, to make permanent electronic recordings of our private communications, there would be no meaningful

> residuum to our right to live our lives free from surveillance. The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communication will remain private. A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning."

Any legislation that infringes citizens' rights to be free of unreasonable search and seizure must be reasonable and demonstrably justified. The onus of proving that a limitation meets that criteria is on the party seeking to uphold the limitation, in this case the Federal Government. As discussed in *R. v. Oakes* [1986] 1 SCR 103 two criteria must be met:

> (1) The objective of the legislation must be sufficiently important, pressing and substantial, "to warrant overriding a constitutionally-protected right"; and
>
> (2) The means chosen must be reasonable, demonstrably justified, and proportional, balancing the interests of society with those of the individuals. With respect to proportionality, the measures must be "rationally connected to the objective", and impair the right "as little as possible". Further, "there must be a proportionality between the <u>effects</u> of the measures… and the objective".

We agree with the Privacy Commissioner of Canada that any proposal that seeks to limit the right to privacy must meet a four-part test:

- it must be demonstrably necessary in order to meet some specific need;
- it must be demonstrably likely to be effective in achieving its intended purpose. In other words, it must be likely to actually make us significantly safer, not just make us feel safer;
- the intrusion on privacy must be proportional to the security benefit to be derived; and
- it must be demonstrable that no other, less privacy-intrusive, measure would suffice to achieve the same purpose.[1]

---

[1] Letter to the Ministers responsible for the "Lawful Access" proposals, November 25, 2002. http://privcom.gc.ca/media/le_021125_e.asp

SUMMARY OF CONCERNS AND RECOMMENDATIONS

Our concerns with the proposals contained in the *Lawful Access Consultation Document* can be summarized as follows:

1. The federal government seeks clarification with respect to the "private" status of e-mail, and suggests that "...[O]ne could argue that e-mail communications, as they are in writing, would not come within the 'private communication' definition."

   We fundamentally disagree. We submit that e-mail is akin to a private oral communication. There is a high expectation of privacy in e-mail, and access to it should be obtained only under the high standard required for current lawful interception orders.

   The future would be bleak indeed if Canadians had to communicate with the awareness that virtually any electronic conversation could be monitored and scrutinized by unseen government officials. Not only would our privacy rights be severely diminished, but our rights of freedom of expression as well.

2. The Consultation Document states that "The public policy objectives of this process are to maintain access capabilities for law enforcement and national security agencies in the face of new technologies and to preserve and protect the privacy and other rights and freedoms of all people in Canada." However, the federal government proposals go beyond maintaining powers for new technology. The proposals greatly increase the breadth and depth of law enforcement agencies' powers to intercept, search and seize the private electronic communications and records of Canadian citizens.

   In many cases, the powers proposed are unprecedented. In others, the powers proposed would substantially lower the threshold that is already required by Canadian law to obtain this information. This lower threshold does not adequately take into account the high degree of privacy that should be recognized in electronic communications and records.

3. The Consultation Document states that "These rapidly evolving technologies pose a significant challenge to law enforcement and national security agencies...as [they] can make it more difficult to gather the information required to carry out effective investigations." However, there is a lack of any empirical or other data that would demonstrate a pressing and substantial need for further law enforcement agency access to private electronic communications and records. There is little if any satisfactory justification given for the new powers proposed.

4. It is doubtful that the new powers proposed would be effective in enabling law enforcement and security agencies to keep up with technological innovations that are constantly being created. Lawbreakers will continue to find new avenues and methods of communication. If Canadians yield to what in fact are endless pressures to increase law enforcement surveillance powers, the result could be a huge loss of privacy in exchange for little gain in safety and security. In our opinion, we have a great deal to lose and not much to gain from the proposals.

5. The proposals in the Consultation Document are so vague in some instances that it is difficult to know what is being proposed. This makes it difficult to assess whether the proposals are reasonable, demonstrably justified and proportional.

We recommend the following:

1. Due to the high expectation of privacy in electronic communications and records, any proposed legislation should require a high threshold for lawful access commensurate with the expectation of privacy in those communications. Lower standards as discussed in the Consultation Document are not appropriate.

   The Criminal Code should be amended to clarify that e-mail, whether in transit or in storage, can be lawfully accessed only under this higher threshold.

2. As a necessary precursor of any legislation in this area, the government should present a well-argued system of privacy protection for private communications, that is not dependent on the form of the communication. The burden should not be placed on the average person to be careful in what he or she communicates because the medium they use determines a greater or lesser privacy status for that communication.

3. The federal government should provide a detailed statement and data with respect to the difficulties faced by law enforcement and national security agencies, so that the proposals for enhanced powers can be reviewed with that information.

4. The federal government should provide draft statutory wording with respect to the proposals, after taking into the account the concerns expressed in this and other submissions.

5. The public should have the opportunity to comment further on revised lawful access proposals, once 2 through 4 above have been completed.

TECHNICAL INFRASTRUCTURE AND INTERCEPT CAPABILITY

The federal government proposes legislation that would require all service providers operating a "transmission facility" to ensure their systems have the technical capability to intercept communications.

The working definition of "transmission facility" is broad and would include wireless, wireline and Internet services. Existing systems would be grandfathered, and the requirement would only apply to new services or when there are significant upgrades to a system. The cost of compliance would be born by the service provider. There would be provisions for forbearance or exemption from the requirements under certain conditions.

Important Note: It is with surprise that we note that there is no provision in the *Convention on Cyber-Crime* that requires states to enact intercept capability legislation. Therefore, this proposal is not based on the Convention or any international requirement. We can only see this as a Canadian-made move for increased law enforcement powers. For all intents and purposes, *intercepts are wiretaps* and must be subject to all the thresholds and protections contained in Part XV of the Criminal Code and established jurisprudence.

Although the Consultation Document states that new services and technologies have "created difficulties", and make it "very difficult" to sustain the technical ability to lawfully intercept communications, no empirical or other data has been provided to adequately explain this. No information has been given as to how many investigations, if any, have been thwarted by cost in time or money because of lack of technical capability. No information is given as to why technical capability is required across all service providers. As a result, there is no evidence with which to assess whether there is a pressing or substantial need justifying this proposal and its effect on privacy rights.

Universities, Colleges, and Public Libraries

The definition of "service provider" is not sufficiently clear in the proposals. If the definition is to include institutions such as universities, colleges, and public libraries, there are serious concerns that such proposals will affect the ability of citizens to conduct anonymous communications and research. These are traditionally open and protected environments. Many libraries have workstations connected to the Internet that do not require IDs and passwords. The computer can be used anonymously. The proposals for data preservation orders and capture of customer name and address discussed below would not only create administrative difficulties for these bodies and its patrons, but also prevent any anonymous communications and research from being carried out. In the end, another important civil liberty would disappear.

We must be vigilant to ensure that increased intercept capability does not equate to a lowering of the standards for lawful access. Lawful access must continue to be obtained only by judicial warrant after a high threshold has been met.

GENERAL PRODUCTION ORDERS

The federal government proposes creation of a "general production order" that would require third parties in possession or control of documents to produce the documents within a specified period of time.

Although there are very limited production orders in the Criminal Code, there is no such thing as a general production order. This is a new power and legal instrument that is being proposed. There is, however, existing provision for assistance orders which enable a judge to order that a person provide assistance in the execution of interceptions, warrants and certain orders.

For all intents and purposes, *production orders are warrants* and must be subject to all the thresholds and protections contained in Part XV of the Criminal Code and established jurisprudence. The federal government does not provide any empirical or other data to justify why a widening of such powers is necessary, or why the present search warrant combined with an assistance order is inadequate

The proposal would put the onus of conducting the search and production of the documents on the third party rather than having the search conducted by the law enforcement agency and assisted by the third party. In the absence of data, it is impossible to assess the justification for this power, and whether it is appropriate to conscript third parties to carry out law enforcement agencies' work.

ISPs should not be Agents of the State

The proposed requirements on ISPs and other telecommunications providers to carry out actions mandated by the state continue a trend to co-opt private companies to become public agents of law enforcement officials. The job of ISPs and other like entities is to provide services for their customers. This should not include monitoring them for purposes of the state.

We disagree with the creation of a general production order. But if such a power were created, the threshold for obtaining one must be high, commensurate with the degree of privacy of the communications and records.

For example, if the order concerns the production of stored e-mail (see discussion below), the threshold should be the same as for the interception of private communications. Production orders must not be used to circumvent the high thresholds that would be required were the law enforcement agency to carry out the search or interception itself.

In addition, general production orders, if enacted, would require terms safeguarding the confidentiality and security of the information gathered for production.

Circumventing International Law Enforcement Procedures

The Consultation Document states that production orders "could also allow law enforcement officials to obtain documents in cases where a search warrant cannot be delivered because the documents are stored in a foreign country". This statement raises concerns as to trans-border search of documents.

A Canadian search warrant cannot by itself be executed outside Canada to obtain documents that are not within the country. In those situations, mutual legal assistance procedures are employed. Production orders would effectively circumvent this procedure and the protections it provides for those within and outside Canada. The proposal is alarming as it raises the possibility of other countries expecting to be able to search computers in Canada with a foreign production order without going through the mutual legal assistance process.

"Anticipatory" Orders

The Consultation Document also asks whether the Criminal Code should "allow for anticipatory orders (e.g., permit law enforcement agencies to monitor transactions for a specified period of time)".

No explanation other than the foregoing sentence is given as to what is meant by this proposal. No definitions of "anticipatory" and "monitor transactions" are given. No explanation or evidence as to why this is proposed is given.

The proposal must be rejected. If "anticipatory" implies that there is not yet sufficient evidence to meet the threshold to obtain an interception order or a search warrant, the proposal is a significant departure from existing law, and an unjustified intrusion of privacy rights. If "monitor transactions" means searching and seizing documents, existing law allows search and seizure under the threshold for judicial warrants. If "monitor transactions" means intercepting real time communication, then existing law allows such interception under Part VI of the Criminal Code, which has higher thresholds. Without more detail from the government it is impossible to comment further.

SPECIFIC PRODUCTION ORDERS FOR TRAFFIC DATA

The government proposes a specific production order in the Criminal Code for "telecommunications associated data" ("traffic data"). A working definition of telecommunications associated data is given and includes "dialling, routing, addressing or signalling, that identifies…the origin, the direction, the time, the

duration or size…the destination or termination of a telecommunication transmission". The government further proposes that the threshold for such an order be the low standard that is currently required for production of telephone records and interception by dial number recorders.

Currently, the interception or search and seizure of traffic data may be ordered under the general warrant or interception provisions of the Criminal Code, both of which have higher thresholds. The proposal therefore calls for a carving out of traffic data from these provisions, and for the threshold for production of traffic data to be at a new lower standard. This obviously provides law enforcement agencies with greater powers of access.

The Consultation Document proposes a lower threshold for traffic data orders because of the "lower expectation of privacy in a telephone number or Internet address, as opposed to the content of a communication". There is a fundamental error in the assumption of this statement. We submit that there is no lower expectation of privacy in an Internet address. To equate telephone numbers with Internet addresses ignores the considerable difference between the amount and quality of information that can be obtained from the two.

Information that can be obtained with an Internet address is far beyond what can be inferred or obtained from a telephone number. If a person telephones a department store to enquire about a product, all that may be recorded is the main number of the store. If the person were to visit the website of the store, and go to the web page of a department and then click on a product, several addresses would be generated, giving far richer information. Similarly, if a search engine is used, the search terms may be revealed in the address. The size of an e-mail may give information. Cellular phone records can identify the general location of the parties to the telephone call.

There is a high expectation of privacy in citizens' Internet and electronic communications. Monitoring this data is akin to video surveillance and interception of private communications. Presently the Criminal Code requires higher thresholds for lawful access for both of these, and that is the standard that should be adopted for an order for production of traffic data. The low standard for dial number recorders is not sufficient to protect the privacy rights of Canadians.

The Consultation Document also 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". No details are given of what this "other data" may be, and it is impossible to comment on this aspect of the proposal, except to say that we fundamentally disagree with the constant theme in the Document that there is a lower expectation of privacy with respect to e-mail and other Internet-based communications.

ORDERS FOR SUBSCRIBER AND/OR SERVICE PROVIDER INFORMATION

The Consultation Document suggests that there could be a specific production order for customer name and address (CNA) and local service provider identification (LSPID). Alternately, it proffers a proposal by The Canadian Association of Chiefs of Police that a national database of subscriber information be created or other existing databases be used to provide this information.

The Consultation Document does not provide satisfactory evidence or what pressing difficulty is being encountered by law enforcement agencies that would justify either of these proposals.

The proposal by the Chiefs of Police to establish a national database of subscriber information essentially amounts to the collection by the state of personal information prior to the commission of an offence, and constitutes an unjustifiable extension of police surveillance into the private domain of communications.

Identity Profiling

Though government can state benign purposes for wanting to aggregate large quantities of personal data, such as informing next of kin in emergency situations, there are many more uses to which such data can be put that are not at all benign. One example that is relevant in the current, post 9/11 political climate is the potential use of such information for “identity profiling”. The aggregation of large amounts of personal data is a prerequisite for government to engage in this controversial practice.

Governments, including Canada’s, are increasingly using modern computer technology for purposes of data matching and data mining to construct profiles of those they think are likely to commit or to have committed crimes. They then take advantage of large pools of personal data to search for individuals who match the profiles. Not only do such programs subject the entire population to surveillance; they also make it feasible to target particular individuals on the basis that they share racial or cultural characteristics, or even political opinions.

CNA and LSPID are personal information. Although this information is often publicly available, it still carries some expectation of privacy. For example, many individuals choose to have unlisted telephone numbers.

Where it is not already publicly available, CNA and LSPID should only be available to law enforcement agencies upon judicial authorization once an appropriate threshold commensurate with the degree of privacy of this information has been met. Law enforcement agencies should not have access to this information prior to meeting that threshold.

The proposal for a national database should also be rejected on the grounds that it is unlikely to be effective or accurate, one reason being that the criminals police hope to identify will use false names and addresses. The proposal would only serve to create a database of law-abiding citizens. Other reasons it would be likely to fail are the libertarian culture of the Internet and the public's well-documented concerns over privacy and security on the Internet.

Recent furors in Canada over the so-called "big brother database" created and then dismantled by the Human Resources Development Agency, and the massive problems of the national gun registry program, provide strong indicators of the likely fate of a national database of subscriber information. Public resentment and resistance toward such a registration regime would almost certainly confound the effort.

DATA PRESERVATION ORDERS

The federal government makes two proposals. The first is provision for "an expedited judicial order" that would require service providers to store and save existing specific data. The data would be preserved "only as long as it takes law enforcement agencies" to obtain a judicial warrant to seize or to produce the data. The purpose of the order would be to provide a "stop-gap" to preserve data that might otherwise be deleted. Secondly, the government proposes that in exigent circumstances, law enforcement agencies should be able to impose a preservation requirement on a service provider without a judicial order, for a specified period such as four days.

Preservation orders do not presently exist in Canada, and their creation would be an unprecedented and unjustified expansion of law enforcement powers.

Again, there is no statement in the Consultation Document justifying the need for these orders. There is nothing to suggest that law enforcement agencies are experiencing difficulties with the destruction or loss of data. Until there is this justification, these proposals should be rejected.

The Consultation Document asks whether a data preservation order should apply not only to stored computer data but to paper records as well. This proposal should also be rejected. The Consultation Document does not identify any problems that have been experienced with the destruction of paper records.

Preservation orders are an exceptional remedy. They should never be used for "fishing expeditions" or as a source or a pool of data that is available should law enforcement agencies ever suspect wrongdoing. If preservation orders are enacted, they must only be available with judicial authorization after an appropriate high threshold has been met, including reasonable and probable grounds to believe that the data sought will be destroyed, lost or modified. The Consultation Document does not set out what threshold is envisioned.

Further, there would have to be specific provisions to:

- prescribe the time limit for preservation orders;
- protect the confidentiality and security of the preserved data; and
- prohibit the disclosure of any of the preserved data unless and until a judicial order for production is obtained.

The time periods suggested by the Consultation Document are not justified. Preservation orders must not become a backdoor to circumvent the high thresholds and judicial authorization required for lawful access.

The government also proposes that in exigent circumstances, law enforcement agencies should be able to impose a preservation requirement on a service provider without a judicial order, for a specified shorter period. We reject such proposal for the foregoing reasons. Further, a preservation order is already "an expedited judicial order".

Finally, although data retention — the routine, longer-term retention of all electronic messages — is not being proposed, we are very concerned that data preservation is the first step towards such a result. Developments on data retention internationally, notably in the EU, may put pressure on Canada to enact such powers. The retention of vast amounts of information including clickstream traffic would be a major expansion in the ongoing assault on privacy.

INTERCEPTION OF E-MAIL

The federal government seeks clarification with respect to the status of e-mail, and whether lawful access to it should be granted under the higher threshold for interception orders required for "private communications", or whether access should be granted under a lower standard required for search warrants.

There is a high expectation of privacy in e-mail and lawful access to it should be obtained only under the high standard for interception orders. E-mail is akin to a private oral communication. The Criminal Code should be amended to clarify that e-mail, whether in transit or in storage comes, can only be accessed under this higher threshold.

SUMMARY AND GENERAL CONCERNS REGARDING THE PROPOSALS

Finally, it is important to view the proposals in the Consultation Document in the context of other legislation that is proposed or has recently been enacted. Privacy rights in Canada are continually under assault, and there has been a chipping away of these rights in the post 9/11 world. The recent anti-terrorist

legislation and Canada Customs and Revenue Agency's program to create a national database on people entering and leaving the country are two recent examples of this disturbing trend.

We must be vigilant to ensure that the right to privacy of Canadian citizens is only limited by such measures that are truly required, reasonable, demonstrably justified, effective and proportionate to the ends to be achieved. The proposals in the Consultation Document show clearly that these requirements have not been met.

We would welcome to the opportunity to comment further on the proposals once further information regarding the necessity of the proposals is provided, and draft legislation has been completed.

Yours Sincerely,

Gerald Fahey
President
BC Freedom of Information
and Privacy Association

This submission has been endorsed by:

Commonwealth Centre for Electronic Governance
Thomas B. Riley, Executive Director

Friends of Freedom
Trueman Tuck, National Coordinator

Muslim Canadian Federation and
Council of the Muslim Community of Canada
Aziz Khaki, Vice President

National Privacy Coalition
Prof. Valerie Steeves, Chair