BY FAX

December 16, 2002

Hon. Martin Cauchon
Minister of Justice and Attorney General of Canada
284 Wellington Street
Ottawa, Ontario K1A 0H8

Hon. Wayne Easter
Solicitor General of Canada
340 Laurier Avenue West
Ottawa, Ontario K1A 0P8

Hon. Allan Rock
Minister of Industry
235 Queen Street
Ottawa, Ontario K1A 0H5

Comments on *Lawful Access – Consultation Document* (August 25, 2002) – OIPC File No. 16763

This letter comments on the above consultation document of the Department of Justice, Industry Canada and the Solicitor General of Canada. That document invites comments on legislative proposals for lawful access by law enforcement agencies to communications and related information.

1.0 SUMMARY

- No evidence has been offered that existing interception and search and seizure laws are inadequate for dealing with electronic communications. Nor does the Cyber-Crime Convention offer a persuasive rationale for the proposals.

- Privacy is a constitutionally protected right. Privacy in electronic communications should give way to law enforcement and national security needs only where those needs clearly outweigh the privacy interest and then only to the minimal extent necessary. There is clearly a reasonable expectation of privacy in e-mail. Existing standards respecting interception of private communications should apply to e-mail interception.

Mailing Address: PO Box 9038, Stn Prov Govt, Victoria B.C. V8W 9A4
Location: Fourth Floor, 1675 Douglas Street
Telephone: (250) 387-5629 Facsimile: (250) 387-1696
Toll Free enquiries through *Enquiry BC* at (800) 663-7867 or (604) 660-2421 (Vancouver)
website: http//www.oipc.bc.ca

- Requiring service providers to acquire the technical capacity to provide lawful access inappropriately co-opts the private sector in state surveillance. The costs to service providers will raise consumer costs and may diminish the competitiveness of the Canadian Internet industry, thus exacerbating concerns about private sector involvement in state surveillance. The development and implementation of Internet technology will be driven by the interests of surveillance and not the needs or realities of Canadian businesses and consumers.

- A specific production order for telecommunications associated data should be available only from a judicial authority applying existing standards and not lower thresholds. Production orders for subscriber or service provider information also should only be available from a judicial authority applying existing standards.

- A data preservation order should be available only from a judicial authority using existing interception standards. Law enforcement authorities should, consistent with s. 487.11 of the *Criminal Code*, only be able to secure preservation when it would be impracticable to obtain a judicial order in the circumstances.

- In the context of creation of a number of surveillance databases in Canada, the proposal of the Canadian Association of Chiefs of Police to create a mandatory-reporting database of all subscribers is worrisome. Final comment is withheld, however, pending further clarification of the proposal and its details.

- Independent oversight of the nature and frequency of use of any new lawful access powers is necessary, recognizing that such oversight must be designed to appropriately protect law enforcement interests.

2.0 DISCUSSION

2.1 Where is the Evidence of Need? – The consultation document says that, for law enforcement and national security agencies, lawful access is an essential tool in the prevention, investigation and prosecution of serious offences and the investigation of security threats. It says telecommunications and computer networks such as the Internet can be used "in the planning, coordination, financing and perpetration of crimes and threats to public safety and the national security of Canada" (p. 3). The paper also says, at p. 3, that

> … rapidly evolving technologies pose a significant challenge to law enforcement and national security agencies that require lawful access to communications and information, as these technologies can make it more difficult to gather the information required to carry out effective investigations.

The paper contends that, in light of the easy flow of information and communications around the world, law enforcement and national security agencies "need modern and effective capabilities to support their investigative or intelligence gathering efforts" (p. 4). For this reason, the document suggests "partnerships with Canadian industry are more important than ever and must be consistently fostered and maintained" (p. 4).

It is striking that the consultation document offers no evidence to support any suggestion that law enforcement or national security activities have been, or could reasonably be expected to be, impaired because existing laws respecting interception or search and seizure are inadequate given present technologies or trends in communication technologies or information flows. In the absence of any persuasive case, based on concrete evidence, that existing Canadian law is inadequate, I question the need for new laws. I am deeply concerned that – bearing in mind that the lawful access proposals are in various respects rather vague at this stage – the proposals weaken existing legal protections for privacy in Canada without a clear and compelling justification.

The contention that changes in Canadian law are necessary so Canada can ratify the Council of Europe *Convention on Cyber-Crime* ("Cyber-Crime Convention") only goes so far. That treaty is encountering very serious resistance, notably in Europe, because of the serious concerns it raises about individual liberty and privacy and because of concerns about the costs to the private sector of implementing treaty-conformed national laws.

In Australia, for example, the Senate has rejected the *Telecommunications Interception Legislation Amendment Act 2002*. In South Africa, the *Interception and Monitoring Act* was abandoned because of public resistance. In recent weeks, officials of the Home Office in the United Kingdom have conceded that the government must begin again with its implementation of the interception and seizure aspects of the much-criticized *Regulation of Investigatory Powers Act*. Among the few countries to have succeeded in enacting laws or implementing proposals comparable to aspects of the Canadian proposals are China, Iraq and Saudi Arabia.

The Government of Canada should only proceed further with the lawful access proposals if a clear evidentiary basis is offered to support the need for changes. To be sure, the Government of Canada should not proceed simply because it is expedient to do so in the post-September 11 climate of fear and insecurity.

Bearing this overriding reservation in mind, the balance of this letter comments on specific aspects of the proposals assuming, only for the purposes of argument, that a need for them has been established on clear evidence.

2.2 Privacy and Electronic Communications – I will first note the constitutional dimensions of privacy in communications and address privacy in e-mail communications.

Privacy and the Canadian constitution

The constitutional dimensions of the right to privacy are beyond debate. The Supreme Court of Canada has on many occasions affirmed that the *Canadian Charter of Rights and Freedoms* affords constitutional protection for Canadians' privacy. For present purposes, I need only quote from the Court's decision in *R.* v. *Duarte*, [1990] 1 S.C.R. 30, at paras. 21 & 22, which relates to interception of communications:

> The rationale for regulating the power of the state to record communications that their originator expects will not be intercepted by anyone other than the person intended by the originator to receive it (see definition section of Part IV.1 of the

> [*Criminal*] *Code*) has nothing to do with protecting individuals from the threat that their interlocutors will divulge communications that are meant to be private. No set of laws could immunize us from that risk. Rather, the regulation of electronic surveillance protects us from a risk of a different order, *i.e.*, not the risk that someone will repeat our words but the much more insidious danger inherent in allowing the state, in its unfettered discretion, to record and transmit our words.
>
> The reason for this protection 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 communications 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. As Douglas J., dissenting in *United States* v. *White*, *supra* [401 U.S. 745 (1971)], put it, at p. 756: "Electronic surveillance is the greatest leveller of human privacy ever known." If the state may arbitrarily record and transmit our private communications, it is no longer possible to strike an appropriate balance between the right of the individual to be left alone and the right of the state to intrude on privacy in the furtherance of its goals, notably the need to investigate and combat crime.

In debate over anti-terrorist and other measures, I have consistently acknowledged that law enforcement agencies and national security agencies should not be hampered in their law enforcement and national security activities by unwarranted concern for individual privacy rights. The balance between state interest and individual rights should only favour state interests, however, where a law or other measure has been shown to be clearly necessary and to intrude on individual privacy only to the least extent practicable. The existing *Criminal Code* provisions respecting interception of private communications appropriately balance individual privacy interests against the public interest in effective law enforcement.

E-mails are private communications

The consultation paper appears to suggest that e-mails are not private communications. It refers to s. 183 of the *Criminal Code*, which defines "private communication" as including any telecommunication or oral communication made under circumstances creating a reasonable expectation of privacy. The paper suggests that this indicates that a written communication is not a "private communication". The paper refers to decisions by some courts that tape-recorded messages, like written letters, are not "private communications" within the meaning of the *Criminal Code* definition, because it is not reasonable for anyone sending a tape or letter to expect that it will remain completely private.

The consultation paper's appeal to the existing *Criminal Code* definition of "private communication", and to court decisions dealing with it, does not advance the analysis. The question remains, should e-mails be regarded as private communications? The obvious and only answer is that e-mails are private communications. The fact that it may be possible for hackers or others to intercept an e-mail using inappropriate technologies or methods does not undercut this. Surely all Canadians regard letters they send to be

private despite the risk that someone will steal them from a mailbox and improperly read them? Such a risk may influence what information is included in private correspondence, but prudence in protecting sensitive information does not mean the correspondence is not a private communication.

The Alberta Court of Appeal has held that there is a reasonable expectation of privacy in e-mail. See *R.* v. *Weir*, [2001] A.J. 869 (affirming [1998] A.J. No. 155). As the trial judge noted in that case, in *United States* v. *Maxwell*, [1995] 42 M.J. 568, the U.S. Air Force Court of Criminal Appeals held, at p. 576, that e-mails carry an objective expectation of privacy, in the following terms:

> However, we find appellant definitely maintained an objective expectation of privacy in any e-mail transmissions he made so long as they were stored in the America Online computers
>
> In our view, the appellant clearly had an objective expectation of privacy in those messages stored in computers which he alone could retrieve through the use of his own assigned password. Similarly, he had an objective expectation of privacy with regard to messages he transmitted electronically to other subscribers of the service who also had individually assigned passwords. Unlike transmissions by cordless telephones, or calls made to a telephone with six extensions, or telephone calls which may be answered by anyone at the other end of the line, there was virtually no risk that the appellant's computer transmissions would be received by anyone other than the intended recipients.

An e-mail should be explicitly recognized by our criminal law as a private communication and should be protected accordingly. Existing *Criminal Code* interception standards should apply and lower standards for interception of e-mails are not desirable. Many of the weaknesses of consultation paper proposals stem from the apparent assumption that e-mail is not a private communication and does not deserve protection as such. Other flaws in the proposals flow from the similar assumption in the paper that data associated with e-mail traffic, Internet addresses and traffic and other such data do not engage privacy interests because they have little or no privacy content.

2.3 Imposing Lawful Access Capabilities – The consultation document suggests that all wireless, wireline and Internet service providers should be required to ensure that their systems have the technical capacity to provide lawful access to law enforcement and national security agencies. This intercept capability would include content and 'telecommunications associated data' (as the latter term is defined in the document).

The proposal to require Internet service providers to meet certain technical standards amounts to forcing businesses to collect and organize data in a manner that is driven by the need to provide lawful access – in the interests of alleged law enforcement needs and state surveillance – rather than a particular business imperative. This could skew business models and the market, not to mention the impact on consumers.

First, I echo the serious concern voiced around the world that imposition of this capability on service providers inappropriately conscripts the private sector as an agent of the state, not a partner, who engages in surveillance for the state. This point is fundamental. Imposition of a technical intercept capability would greatly blur the line

between surveillance activities of, or on behalf of, the state and commercial surveillance. Creation of a surveillance state is, of course, to be avoided at all costs, but that is precisely the direction in which this proposal tends.

Second, such a proposal carries grave cost implications for service providers, especially Internet service providers. The bursting of the Internet bubble may have set back electronic commerce, but it did not destroy it. Imposition of a costly lawful access capacity requirement will almost certainly further inhibit electronic commerce. Have such risks and benefits of imposing such a lawful access requirement been assessed? In the Netherlands, for example, cost implications for Internet service providers have been so significant that the government has been forced several times to postpone the deadline for compliance with a technical intercept capacity requirement legislated a few years ago. Similar concerns have been expressed, and difficulties encountered, in the United States under the 1996 *Communications Assistance to Law Enforcement Act.* European Union countries have encountered stiff resistance from service providers on this very issue.

While these cost implications do not directly affect privacy interests, I am concerned that the end-result could be to cause consolidation in the Internet service industry. Such a consolidation would reduce competition, could affect service levels and certainly would exacerbate concerns about private sector surveillance on behalf of the state. Moreover, this proposal would amount to state policy regarding law enforcement and surveillance driving development and application of technology, not the market.

2.4 Production Orders – The consultation document indicates that several types of production orders are being considered for enactment: a general production order, a specific production order for traffic data and a specific production order for subscriber or service provider information (or both). By production order, the document means an order that would compel service providers to produce information to law enforcement agents within a set period.

As I understand it, a general production order would be similar to a search warrant, the salient difference being that a production order would require the service provider to deliver documents to a law enforcement agency or make them available to that agency. In the case of a search warrant, of course, law enforcement agents enter relevant premises to find and take away all material covered by the warrant.

The following comments focus on the proposed specific production orders. At the very least, in each instance I believe that existing legal standards must be preserved. No case has been made for lower standards. As regards the paper's reference to "anticipatory orders", the concept is not fleshed out, so I cannot comment.

Specific production orders for telecommunications associated data

The consultation document proposes, at p. 11, that a specific production order should be available "under a lower standard" than existing *Criminal Code* thresholds for telecommunications associated data, supposedly because Internet traffic data is comparable to telephone number records and dial-number recorders.

I strongly disagree with the paper's assumption that there is a lower expectation of privacy in relation to Internet traffic data, comparable to telephone number-related records and dial-number recorder data. The proposed definition of telecommunications associated data would, in the context of e-mail and Internet use, appear to enable law enforcement agents to obtain the following data: e-mail sent-to and received-by addresses; computer IP addresses; data respecting duration of communications; data as to date and time of communications; data about the size of a communication; data disclosing websites visited; and, possibly, data as to e-mail subject line and attachment file names.

By contrast, dial-number recorders merely record identifying information about telephone numbers called from a specific telephone number, not call-content information or other potentially sensitive information of the kinds I have just described. Further, in the case of wireless telephones, which would be covered by the lawful access proposals, unit location information would be in issue, this distinguishing such data from dial-number recorder data.

The reality is that telecommunications associated data can yield a rich lode of information using data-mining and other techniques to disclose information about the intimate details of Canadians' personal lives. Any analogy between dial-number recorders and telecommunications associated data should be rejected and specific production orders for such data should only be available applying existing *Criminal Code* standards. I also note that, before enactment of s. 492.2 of the *Criminal Code*, the Ontario Court of Appeal ruled that use of dial-number recorders to obtain local call information without prior judicial authorization contravened the *Criminal Code* prohibition against interception of private communications. See *R.* v. *Griffith* (1988), 44 C.C.C. (3d) 63. Canadian courts were not unanimous in this view, but the fact remains that the Ontario Court of Appeal and other courts across the country considered even dial-number recorders to be problematic in the absence of any legislated protections for privacy.

The document also proposes, rather obscurely, that a specific production order should be available under a lower standard for unspecified "other data or information in relation to which there is a lower expectation of privacy" (p. 12). It is not possible to comment usefully on this proposal in the absence of better information as to what is intended.

Production order for subscriber and service provider information

The consultation paper notes that law enforcement authorities must get "some form of court order" to obtain subscriber or service provider information where that information is not voluntarily disclosed to them by its custodian. The paper also acknowledges that basic customer information has traditionally been made available to law enforcement officials. Yet it is suggested that a specific production order could be made available even if no investigation is under way and according to an unspecified lower threshold.

I am concerned that the case for such orders has, again, not been made out. If law enforcement agencies have traditionally been able to get such information it is not clear to me why authority to compel it is needed. Certainly, if custodians have historically delivered such information to law enforcement agencies to assist existing investigations,

I have reservations about allowing compelled disclosure in non-investigative situations. I am, therefore, skeptical about the need for this proposal, at the very least, and would want to see more detail before commenting further.

2.5 Data Preservation Orders – As the consultation document indicates, the Cyber-Crime Convention contemplates a new tool, called a preservation order. Such orders require service providers to retain and preserve data for as long as it takes a law enforcement agency to obtain a warrant to seize the data or a production order requiring its delivery to the agency.

I am not opposed in principle to this proposal. I accept that, because of the nature of electronic data, it may be necessary for law enforcement agencies, in limited cases, to be able to obtain a preservation order to give them time to apply for a warrant or production order from the appropriate judicial authority. The standards to be applied in obtaining such an order from a judicial authority should ideally be comparable to existing standards. The standard of reasonable grounds to believe an offence has been or may be committed may be one approach to examine.

This is not to say that I support the breadth of the proposals found in Articles 16 and 17 of the Cyber-Crime Convention. To the contrary, I believe those articles are excessively broad. I am also concerned that the 90, 120 or 180-day retention periods mentioned in the consultation paper are excessive. If any preservation order provision is enacted, it should apply only to stored computer data (not paper records), it should be available only in the context of an ongoing investigation into a possible violation of a criminal law and preferably should be available only from a judicial authority applying the criteria of reasonable grounds.

As regards exigent circumstances, where not even a preservation order pending warrant can be obtained, law enforcement authorities should at most be empowered to require a service provider to preserve information only where, consistent with s. 487.11 of the *Criminal Code*, obtaining a judicially-issued preservation order "would be impracticable" in the particular circumstances. It is worth underscoring here my concern that no evidence has been presented whatsoever that this or any of the other proposals is needed because existing laws are inadequate.

The fine line between data preservation orders and legislated data retention requirements must be acknowledged. The latter concept is even more troubling, of course, since it entails creation of massive surveillance databases. For example, in the United Kingdom a one-year retention period for data has been imposed. Apart from the civil liberties concerns data retention raises, one wonders about its efficiency or efficacy. The cost implications are enormous. In a December 12, 2002, ZDNet article, America Online is reported as estimating, in testimony before an all-party Parliamentary inquiry in the United Kingdom, that its setup costs alone to comply with United Kingdom law are roughly £30million, with the same again in running costs. That is the cost for just one Internet service provider. The cost implications of data preservation orders also cannot be underestimated, but certainly data retention requirements should be avoided at all costs.

2.6 National Database of Subscriber Information – I have serious reservations about the proposal of the Canadian Association of Chiefs of Police for establishment of a national database of subscriber information. In addition to the concern that this would also conscript the private sector into surveillance, the creation of such a centralized database must be viewed in light of other database proposals either under way or on the table. I refer here, as an example, to the Canada Customs and Revenue Agency's air traveller database, about which I have previously expressed grave concern.

The proliferation of such databases is deeply troubling. Now more than ever such proposals must be subjected to close scrutiny before they proceed. Failing clear evidence that a national database of subscribers is necessary because existing means of collecting subscriber information are inadequate, or that such a database would actually work and not be circumvented by criminals, I believe the proposal should not be pursued at this time. At the very least, if the proposal proceeds, concerns about accountability and independent oversight are critical and must be addressed.

2.7 Accountability – Nowhere does the consultation paper indicate that accountability measures are being contemplated. If new and broader powers are enacted, and I again suggest the case for them has not been made, a system of accountability is needed. This of course cannot be allowed to jeopardize law enforcement or national security interests, but independent oversight of the frequency and nature of use of new powers is necessary. A body such as the Security and Intelligence Review Committee should be considered in relation to any new law enforcement access to e-mail and other electronic communications data, bearing in mind my concern that the case for the proposed powers has not been made.

Yours sincerely,

ORIGINAL SIGNED BY

David Loukidelis
Information and Privacy Commissioner
for British Columbia

cc: Lawful Access Consultation
Criminal Law Policy Section
Department of Justice

George Radwanski
Privacy Commissioner of Canada

Provincial & territorial privacy commissioners and ombudsmen