Electronic Privacy Information Center (EPIC)
Washington, DC

Comments submitted in consideration of the Canadian Government's "Lawful Access – Consultation Document" of August 25, 2002

(December 16, 2002)

Introduction

On August 25, 2002, the Canadian Department of Justice, Solicitor-General and Industry Canada released a document entitled "Lawful Access – Consultation Document" (the "Consultation Document") which proposes to amend several Canadian statutes, including the *Criminal Code* and the *Competition Act*, in consideration for the ratification of the Council of Europe *Cyber-Crime Convention* (the "CCC").

The Canadian government's discussion paper proposes requiring all providers of Internet, wireline and wireless services to add surveillance capabilities to their networks to allow police and security agencies to monitor on users' communications (mobile and landline phone calls, e-mails, Internet browsing, etc.)

The purpose the government intends to address with this Consultation Document is the evolution of modern telecommunications and computer networks such as the Internet. Such technologies, according to the government, "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."[1]

The Consultation Document has raised strong opposition by the telecommunications and ISP industry (especially because of costs of compliance issues), privacy watchdogs and civil society (because of the unjustified increase in the level of electronic surveillance) and Internet users and concerned citizens (because of their sense of a general loss of privacy). Some of the changes the Canadian government wishes to introduce may have a major impact upon important constitutional values and rights, such as the freedom of speech and the right to online privacy and anonymity.

[1] Department of Justice, Industry Canada, Solicitor General Canada, "Lawful Access – Consultation Document", August 25, 2002, http://www.canada.justice.gc.ca/en/cons/la_al/.

EPIC welcomes the opportunity to make comments on the issue of lawful access. EPIC supports many of the recommendations expressed by Canadian civil liberties groups. We therefore respectfully recommend that the Department of Justice, Industry Canada and Solicitor General Canada address civil society's concerns and recommendations.

1. The Consultation Document's Main Issues of Concern for the Civil Society

As a general concern, civil society appears to agree that the Consultation Document lacks justification for the proposed lawful access measures, and does not include counter-balancing measures that sufficiently protect the public interest and prevent misuse of the proposed new powers.

The Canadian civil society has addressed the following issues as raising most concern:

- New investigatory powers for law enforcement authorities may be exercised under lower judicial standards than those currently applied to search and seizure warrants and intercepts under the *Criminal Code*;
- Telecommunications and Internet service providers would have to make their network "wiretap" compliant;
- Broad and general surveillance measures of electronic communications and the establishment of a national subscriber database are a serious threat to online users' right of anonymity;
- The distinction between traffic, location and content data is unclear. The Consultation Document negates the expectation of privacy individuals can have with respect to their traffic data;
- The legal status of e-mail is unclear, especially with regard to its treatment for interception purposes.

2. Summary Review of the Consultation Document and EPIC Recommendations

A. The Consultation Document does not address all of CCC's new obligations and its consequences for individuals' rights.

The Consultation Document does not discuss several of the issues raised by the Cyber-Crime Convention. This is, for example, the case with assistance orders for disclosure of encryption keys, and new criminal offences for commercial copyright infringement, child pornography, real-time monitoring of communications data, etc. As the CCC's obligations go much further than the Canadian proposal, the Canadian government should not wait till later to incorporate all of the international treaty's obligations into the law. Otherwise, data preservation orders, already provided for in the Consultation Document, could be used for other purposes like investigations related to alleged copyright infringements, such as peer-to-peer file sharing on the Internet. The CCC also provides for mutual assistance between countries. What would happen to a Canadian citizen being the subject of an investigation by a country such as Albania (that has recently

ratified the CCC) in a case where the police request his data to be preserved? The CCC would generally compel Canada to make the request to their own police on Albania's behalf[2].

EPIC therefore recommends that:

> The Consultation Document should address all the Cyber-crime Convention's obligations, including its protections for individuals' rights, before starting to implement that convention into national law.

B. The Consultation Document does not demonstrate by empirical evidence why legal changes are actually needed by law enforcement authorities.

The proposal only justifies the changes by the need to comply with the CCC. There is no objective criteria to show that law enforcement needs new powers as they have not been able to demonstrate that they are not currently able to complete investigations due to lack of technological or legal ability. While civil liberties groups have repeatedly asked for statistics on authorized search and seizures/wiretaps, they were only shown statistics on warrants/intercepts requested, but not how many were not completed for lack of ability.[3]

EPIC therefore recommends that:

> The Canadian government and law enforcement should first assess whether their current technological capabilities or laws have prevented them to solve the crimes they specifically target as requiring the enactment of new lawful access regulations. If, and only if, their current powers do not provide adequate law enforcement tools, would the change in lawful access provisions be justified. This requirement would apply for each and every crime the government requests new investigation tools and laws for.

C. The justification of the new lawful access measures by reference to recent technological developments is not convincing.

While broader lawful access measures may be legitimized due to new technological developments that can affect the efficiency with which law enforcement may pursue criminal investigations, the Consultation Document does not offer any assessment of the nature and scope of the problem, and does not demonstrate the effectiveness of the new lawful access provisions. As an example of such concern, the Document does not address how the use of encryption may defeat the intent of the proposed new surveillance schemes. Considering that most criminals

[2] The Canadian government could refuse only if it considers the request to be related to a political offence or if the request is likely to prejudice the government's sovereignty or security. (CCC, Article 27 (4) (a) & (b)).

[3] Cfr M. Geist, "Federal proposal tell only part of cybercrime story", *The Globe & Mail* (October 3, 2002); Privaterra Project, Comments submitted to the Department of Justice, the Solicitor-General and Industry Canada in consideration of the Council of Europe Convention on Cyber-crime and the Lawful Access Consultation Document (November 21, 2002).

probably have recourse to strong encryption, the persons most affected by broad and general surveillance schemes would be law-abiding citizens.

EPIC therefore recommends that:

> Other options should be considered that mitigate the consequences of the new lawful access provisions on Canadians' freedom of speech and presumption of innocence.

D. New investigatory powers for law enforcement authorities would have to be exercised under lower judicial standards than those currently applied to search and seizure warrants and intercepts under the *Criminal Code*.

The Consultation Document calls for the creation of several new production orders that could be used by law enforcement to compel ISPs to disclose certain information by having only to meet low evidentiary standards.

These new investigation powers include:

- Mechanisms for providing subscriber and service provider information to law enforcement;
- The creation of a new data preservation order that could be used to compel ISPs to preserve all data related to a client or a transaction for a certain period of time while an investigation is under way.

EPIC therefore recommends that:

> If new investigatory powers for law enforcement are indeed required, they should be under established judicial standards that meet the same tests as those for warrants/intercepts (i.e. subject to independent judicial oversight).
>
> The principle of preserving communications data should be implemented only if the government is able to prove that not preserving data for a certain time would severely affect their efficiency in conducting investigations.
>
> The scope of a preservation order should be limited to:
> a) a specific offence or suspicion that an offence has been or will be committed; and
> b) the preservation order should last only as long as necessary to execute a warrant.

E. Telecommunications and Internet service providers would have to make their network "wiretap" compliant to law enforcement and national security agencies.

ISPs would have to provide authorities with access to all communications over their networks, including the content of messages and details of data traffic.

The new interception tools that ISPs and telecommunications companies would have to install on their networks would provide law enforcement agencies with the opportunity to collect vast amount of content information that it would not be able to collect under any circumstances in the offline world. The justification of the distinction between law enforcement monitoring capabilities of online and offline content is nowhere to be found in the Consultation Document. Moreover, law enforcement authorities can hardly justify why they need to be able to collect all online content information while they cannot do it for regular mail. People do not have different and lower expectations of privacy with regard to the e-mails they send on the Internet than with respect to the letters they write.

There is another danger raised by the establishment of a mandatory interception regime in favor of law enforcement with respect to all messages sent by all of ISP and telephone companies' customers. Once all this data is stored, it will be easy for law enforcement to push for wider and broader preservation capabilities and obtain, later and with the proper legal authorizations, wide data retention capabilities. While, until now, the Canadian government only considers data preservation, growing proposals by the European Council for harmonized EU data retention schemes, coupled with the implementation of new law enforcement tools proposed in the Consultation Document, could easily facilitate a shift into a data retention policy at a later stage.

The Consultation Document also raises serious security issues since the existence of omnipresent interception capabilities would make it more tempting and easier for criminals to break into the vast databases of content information stored by ISPs and telephone companies.

EPIC therefore recommends that:

> Compelling ISPs and telecommunications companies to establish an infrastructure capability that could provide access to the entirety of communications over their networks has not been adequately justified in the Consultation Document; infringes upon people's expectation of privacy, could very easily lead to broad and mandatory data retention regimes in the future, and raises serious breach of security issues. For the foregoing reasons, the government's requirement on service providers to ensure intercept capability should not be implemented.

F. Compatibility of new lawful access provisions with Canada's data protection laws.

The Consultation Document does not articulate data protection requirements while it lowers the legal standard for intercepting and preserving communications; provides for new investigation tools for law enforcement agencies; burdens ISPs and telecommunications companies with new and heavy technical requirements; and facilitates the release of customer name and address ("CNA") and local service provider identification ("LSPID"). It is also apparent to civil society groups that various parties may seek access to the information collected by service providers for reasons other than the original purpose for which they were collected and preserved. For those reasons, it does not appear that the Consultation Document has sufficiently taken into account the implications of the new measures for data protection.

EPIC therefore recommends that:

> The Consultation Document should specifically address privacy issues in each instance where there is a risk for individuals' privacy. It is not enough to refer generally to the *Charter of Rights and Freedoms* protections, the *Privacy Act* or the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). Instead, the government should ensure that businesses and individuals are not intruded upon unnecessarily and that the collected data will be adequately protected, managed, and deleted after a specific period of time, and will not end up in other databases for secondary use and monitoring for different purposes. These are specific legal obligations that should be set out in the Consultation Document.

G. The distinction between traffic, location and content data is unclear.

Packet-mode communications often contain both traffic data and content data. The distinction between location and traffic data as opposed to content data is difficult to assess. The nature of data changes the debate about interception, production and preservation orders since the information collected from such data is much more revealing of an individual's private life than simply his or her name, address and telephone number. Unlike analog communications, digital traffic and location data from electronic communications and networks contain more information about individuals than ever before. Some traffic data, because it has the potential to reveal many details about one's lifestyle, political and religious opinions, sexual life, and intimate relations, is subject to the highest constitutional protections, particularly in the criminal investigation context. On the other hand, it has been shown that investigatory tools for packet-mode communications cannot separate traffic and content data.[4]

EPIC therefore recommends that:

> All traffic data should be generally subject to the highest constitutional protections because of the reasonable expectation of privacy they attract. Further, as law enforcement has not been able to prove that their investigatory tools could successfully separate content and traffic data, both types of data should be guaranteed the same level of constitutional protection, unless the traffic data in question comprises only information that law enforcement would normally expect to receive from an intercept of a traditional analog service.

H. The legal status of e-mail is unclear, especially with regard to its treatment for interception purposes.

Civil society is generally of the opinion that people e-mailing each other should benefit from the same level of protection as people using regular mail and the telephone. Intercepting or

[4] For a detailed analysis of this issue, see Privaterra Project, Comments submitted to the Department of Justice, the Solicitor-General and Industry Canada in consideration of the Council of Europe Convention on Cyber-crime and the Lawful Access Consultation Document (November 21, 2002).

accessing e-mail at any point during the transmission between sender and recipient should be an offence unless access to it is authorized by a search warrant or subpoena or another legal instrument.

EPIC therefore recommends that:

> E-mail should attract the same reasonable expectation of privacy as accorded to first-class mail. The status of an e-mail communication (i.e. whether it is "in transit" or stored), should not determine the protection accorded to it in law.

I. The establishment of a National subscriber database is not warranted and threatens the right to anonymity.

The establishment of a national database including all online service and telephone users' name and address information would be a disproportionate measure when assessing it with law enforcement's objectives of investigating crimes and prosecuting criminals. Many civil society organizations assert that Canadians have the right, although not absolute, to anonymity. There is no reason why online activities and expression should be less private than the same activities and expression in the 'offline world'. The possibility for the industry and law enforcement to match everyone's online activities with his or her identity in real life presents too many risks for people's privacy.

It would also, and on a purely practical perspective, be impossible to build a comprehensive national subscriber database as some online service providers never require authentication from their users.[5] If criminals wished to avoid inclusion in such a database and detection by law enforcement authorities, they could use such providers' services.

EPIC therefore recommends that:

> Anonymity online should be protected in the same way anonymity is in regular mail correspondence.

J. A set of new offences has to be created to counterbalance law enforcement's new powers.

New offences counterbalancing law enforcement's new powers would protect the public from potential police abuse and misuse of investigatory materials[6]. Such offences may include seeking access to electronic communications without an Order to Produce or similar legal instrument; collecting electronic communications without a legal instrument allowing the

[5] This is the case, e.g., of online virtual communities and free web-based e-mail services.

[6] Defined as "electronic communications that are intercepted, stored and disclosed to a law enforcement agency under the authority of a search warrant, Order to Produce, or other legal instrument." Cfr Canadian Information Processing Society, Comments on the Consultation on Lawful Access, p. 3 (November 15, 2002), http://www.cips.ca/it/position/lawful (last accessed: December 12, 2002).

organization to do so, etc., with penalties similar to those under the Personal Information Protection and Electronic Documents Act.[7]

K. Civil society organizations should be more involved in the legislative procedure.

Civil society's ability to provide feedback has been limited due to a lack of detail and clarity regarding the legislative proposals or even the issues they are intended to address.

EPIC therefore recommends that:

> If regulations for service providers are drafted at some later stage, the government should be more open, and civil liberties interests should be more taken into account by opening the debate to civil society representatives.

L. Lawful access measures, while aimed at deterring criminal activity, may also limit one of the fundamental goals for which the Internet was created: to be a vehicle for promoting democracy, online activism, and the free exchange of ideas.

If the public believes that ISPs could readily release information about their online activities, they may be less likely to engage in human rights campaigns or legitimate public protest. The government must make clear to the Canadian public that it is not using the current climate of fear over terrorism as a pretext for enhancing its present and future surveillance capabilities without legitimate need.

EPIC therefore recommends that:

> The government has to provide more detailed information about the law enforcement and intelligence community's needs for lawful access. It should demonstrate that all new proposed surveillance powers are proportionate to the objectives it seeks to reach. The government also should engage in more consultations with the civil society to enhance trust, build dialogue and promote democratic governance.

3. EPIC Supports Canadian Civil Liberties Groups' Concerns About the Government's Lawful Access Consultation Document

For the arguments outlined above, EPIC reaffirms its general support of Canadian civil liberties organizations in their contention that the lawful access proposals, in their current form, are not proportionately tailored to address real and perceived impediments to law enforcement in the

[7] See Canadian Information Processing Society, Comments on the Consultation on Lawful Access, p. 3 for more information.

face of "rapidly evolving [communication] technologies".[8] Nor do they contain enough safeguards to counter-balance new implications for constitutional rights and freedoms.

EPIC further proposes:

- All future legislative proceedings surrounding the implementation of the CCC should be open to the civil society to allow them to provide comments and input. In that regard, the government, when drafting lawful access "regulations"[9] with the industry should give civil society the possibility to voice their concerns and issue recommendations.

- The new powers the Canadian government intends to create for law enforcement authorities should not be available for "fishing expeditions" and purposes unrelated to the concerns that originally justified their creation.

Respectfully submitted,

_____

Marc Rotenberg
Cédric Laurant
Electronic Privacy Information Center
1718 Connecticut Ave. N.W., Suite 200
Washington, DC 20009
United States of America
+1 202 483 1140 (tel)
+1 202 483 1248 (fax)

[8] "Lawful Access – Consultation Document", p. 3.
[9] As referred to in the "Lawful Access – Consultation Document", p. 8.