TABLE OF CONTENTS

Page

CANADA

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

TELECOMMUNICATIONS AND LAWFUL ACCESS: I. THE LEGISLATIVE SITUATION IN CANADA

INTRODUCTION

"Lawful access" is an investigative technique used by law enforcement agencies and national security agencies(1) that involves intercepting communications(2) and seizing information (during a search) where authorized by law. Canada, unlike other countries,(3) suffers from a legislative void in th

THE PROBLEM POSED BY NEW TECHNOLOGIES

Canadians have access to an ever-growing number of new communications technologies. More than half of all households have a cell phone and Internet access at home.(5)

According to law enforcement agencies, new technologies such as wireless data networks and voice over Internet protocol(6) often present obstacles to the lawful interception of communications.(7) Such technologies can create "intercept safe havens" where criminal groups are able to operate without being detected. In light of factors such as deregulation of the telecommunications market, the growing complexity of telephone networks makes investigators' work more difficult and results in delays in identifying suspects.

Since 1995, the Canadian Association of Chiefs of Police (CACP) has been calling for legislation to compel all telecommunications service providers to ensure that they have the capability to enable police services to carry out interceptions on their networks.(8) While this reform initiative began in the 1990s, the attacks of 11 September 2001 probably highlighted the issue and the need for a bill to more effectively combat terrorism(9) and organized crime.

On 23 November 2001, Canada signed the Council of Europe's *Convention on*

new technologies.[11] Because international cooperation is essential to address an area in which crime knows no borders, the treaty also aims to facilitate information-sharing among different countries' law enforcement agencies.

After a strategic framework was developed in 2000, representatives of Justice Canada, Industry Canada and the Solicitor General of Canada held public consultations, from August to December 2002. Over 300 submissions were received, from police services, industry, civil rights groups and individuals. A summary of the results of the consultations was released in 2003. This was followed by a series of meetings with stakeholders in 2005.

On 15 November 2005, the Minister of Public Safety and Emergency Preparedness tabled Bill C-74 in the House of Commons. The proposed Modernization of Investigative Techniques Act dealt with certain very specific aspects of the rules governing lawful access, and had two objectives:

•

and the *National Defence Act*.[15] The bill would have maintained the powers conferred on law enforcement agencies by those Acts but would have enabled the agencies to exercise them regardless of the technology used by telecommunications service providers (interception capability). It also provided for certain agencies to have access to basic information relating to telecommunications service subscribers (subscriber information).

A. Interception Capability

At present, there is no Canadian legislation compelling all telecommunications service providers to use apparatus that is capable of intercepting communications. Only licensees that use radio frequencies for wireless voice telephone services[16] have been required, since 1996, to have facilities that permit such interceptions.[17] There is no similar legislation for other telecommunications service providers.

It was this absence of standards relating to the interception capability of telecommunications service providers that the bill was designed to remedy. It would have required all service providers – for example, Internet service providers (ISPs) – to possess apparatus that would enable law enforcement agencies to intercept communications sent to a service provider, after a judicial authorization had been obtained. The bill therefore applied, subject to specified exemptions, to all telecommunications service providers that operate a transmission facility in Canada.[18]

Moreover, the requirement for uniform interception capability related both to transmission data and to the actual content of the communication. An ISP would therefore have had to use apparatus that enabled law enforcement agencies to identify, for example, on the one

(15) R.S. 1985, c. N-5. The *Competition Act* (R.S. 19m

hand, subscribers' e-mail and Internet protocol (IP) addresses, the date and time of communications and the type of file transmitted (transmission data) and, on the other hand, the Web pages visited and the substance of messages (content-related data).(19)

Once a law enforcement agency had obtained a judicial authorization, the telecommunications service provider would have had to comply with any request relating to the interception of communications. Under the regulations policy adopted by the Department of Public Safety and Emergency Preparedness, the telecommunications service provider would have had to allow law enforcement agencies to intercept communications as soon as possible after receiving a written or oral notice.(20)

In addition, the telecommunications service provider would have been legally required to:

- provide assistance to any law enforcement agency to permit it to assess telecommunications facilities;(21)
- prepare a list of the names of its employees capable of providing assistance and make it

- be able to separate the communications of the person for whom the authorization is granted from those of other users and to isolate the transmission data from the data relating to the meaning of the communication;
- correlate and link the traffic data to the content of an intercepted communication so that the law enforcement agency could, for example, establish a connection between the offence committed and an IP address;
- allow law enforcement agencies to intercept the communications of many users that are sent at the same time;
-

Because requests must relate to specific individuals, the designated persons would have been required to provide at

•

telecommunications service provider produces the information requested. Law enforcement agencies can thus obtain documents that are located in another country. The production order can be general, that is, it can apply regardless of the type of information sought,[39] and in that case is issued based on the existence of reasonable grounds for *believing* that an offence has been committed (stringent test).[40] It can also be specific, for example, in order to obtain a record of telephone calls,[41] and in that case is issued based on the existence of reasonable grounds for *suspecting* that an offence has been or will be committed (less stringent test).[42] A proposal was made during the 2002 consultations to create a production order to obtain information from service providers showing telecommunications traffic data.[43] Like an order relating to records of telephone calls, the proposed production order could have been made on the basis of the less stringent test: the presence of reasonable grounds for suspecting.[44]

- *Electronic mail*: The bill did not resolve the debate regarding how electronic mail should be treated. It did not specify which rules apply to electronic mail: Part VI of the Code[45] or the provisions relating to search warrants.[46] The Part VI rules are more stringent than those relating to search warrants.[47] Part VI allows police services to intercept a "private

(39) Section 487.012 of the Code. The *Competition Act* also provides for such an order (par. 11(1)(*b*)).

A. Law Enforcement Agencies

During the consultations, law enforcement agencies generally supported the lawful access proposals. They were of the view that there must not be "safe havens" in Canada where it was impossible to intercept communications, and that a service provider that failed to meet the obligation to guarantee interception capability should be liable to a large fine.

With respect to the subscribers' names and addresses, law enforcement agencies did not regard these as personal information. They thus agreed that they should be able to have access to them without a warrant or court order. They also advocated the creation of a national database containing this type of information.

B. Telecommunications Industry

While the industry generally supported the idea of permitting effective lawful access in the face of technological change, some doubt was expressed as to the need for the bill:

- *Necessity for the bill*: Industry representatives questioned the need for the bill, in the absence of any evidence that investigations had failed because of inadequate technical interception capability.
- *Cost*: The question of the cost associated with implementing a standard interception capability was of particular concern to telecommunications companies. They also argued that providing lawful access services to law enforcement agencies, such as providing subscriber information and assisting them in interception procedures, would generate high ongoing costs in terms of personnel, training and security.(52) If the government did not offer reasonable compensation, those costs would have to be borne by consumers. A group composed of telecommunications companies and representatives of police services suggested that the money confiscated from criminals be used to fund the new lawful access measures.(53)

(52) Campbell Clark, "Ottawa demands greater wiretap access," *The Globe and Mail* [Toronto], 11 October 2005, p. A1.

(53) Jim Bronskill, "New proposal would have criminals foot wiretap bill: Controversial law could be introduced next month,"

- *Technical requirements*: Companies opposed the establishment of technical interception requirements that are unique to the Canadian market.[54] Given the differences in the size of the markets, Canadian companies would have had to bear higher costs. Some associations[55]

In addition, intercepting an Internet communication can reveal a lot more personal information than wiretapping a telephone conversation, and therefore calls for a different approach to be taken. Moreover, the new measures regarding lawful access might engender public distrust of new technologies by reinforcing the belief in constant surveillance by "Big Brother."

When someone's name or address is combined with a unique identifier such as a telephone number, the rules that protect privacy should come into play. Existing legislation that offers that protection should not be amended in order to gain access to this kind of information without a warrant.

D. Civil Society Groups[59]

In the view of the civil society groups, the consultation document was unconvincing on how the measures would actually help fight terrorism or organized crime. In that respect, it was pointed out that there were no statistics to support new lawful access legislation. As an alternative to the imposition of new obligations, law enforcement agencies should instead be given the technical expertise and equipment they need to deal with changes in the nature of crime and in technology.

As well, given that the technical requirements for interception would apply only when systems are upgraded, this could amount to a disincentive to improve equipment and services. Some service providers might prefer not to update their systems so that they would not be compelled to meet the new standards.

The question of subscriber information was also problematic. Law enforcement agencies should still have to obtain a warrant or court order in order to get access to such information. The protection measures provided in the bill were not sufficient.[60]

E. General Public

Here again, the question was raised as to what urgent need the lawful access ere no statis

The protection measures that apply to requests for subscriber information were insufficient, and measures should be implemented prior to information being disclosed, not just once the law enforcement agency had actually obtained the information requested.

There were also concerns that the new obligations would ultimately result in higher charges for users.

CONCLUSION

Bill C-74, which died on the *Order Paper* on 29 November 2005, was developed following extensive consultations. It responded to the concerns of law enforcement agencies and national security agencies, which stated that new technologies often represent obstacles to the lawful interception of communications.

The bill would have allowed law enforcement agencies to intercept any communication legally, regardless of the technology used to transmit it, and would have set up an accelerated procedure to allow law enforcement agencies to gather information on a subscriber to a telecommunications service without a warrant or court order, subject to certain protection measures.

The bill was intended as a key step in the harmonization of legislation at the international level, particularly with regard to the interception capability of telecommunications service providers. This type of requirement is found in the legislation of a number of other countries – notably the United States – which are taking action to combat terrorism and which, like Canada, have signed the Council of Europe's *Convention on Cybercrime*.

Further information on the legislative situation in the United States and two other countries can be found in the previously mentioned companion publication, a comparative study of telecommunications and lawful access in these countries.[61]

(61) Valiquet (2006).