PRB 05-66E

Library of Parliament Bibliothèque du Parlement

TELECOMMUNICATIONS AND LAWFUL ACCESS: II. THE LEGISLATIVE SITUATION IN THE UNITED STATES, THE UNITED KINGOM AND AUSTRALIA

Dominique Valiquet
Law and Government Division

28 February 2006

PARLIAMENTARY INFORMATION AND RESEARCH SERVICE
SERVICE D'INFORMATION ET DE RECHERCHE PARLEMENTAIRES

TABLE OF CONTENTS

Page

CANADA

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

TELECOMMUNICATIONS AND LAWFUL ACCESS: II. THE LEGISLATIVE SITUATION IN THE UNITED STATES, THE UNITED KINGOM AND AUSTRALIA

INTRODUCTION

This is the second of two documents dealing with "lawful access,"[1] an investigative technique used by law enforcement agencies and national security agencies.[2] It involves the interception of communications[3] and seizure of information (during a search), where authorized by law.

Shortly before the dissolution of the 38th Parliament, the Minister of Public Safety and Emergency Preparedness introduced a bill (which later died on the *Order Paper*) on an issue of importance for Canada: "wiretapping" in the era of new technologies. Bill C-74, the Modernization of Investigative Techniques Act – the first legislative proposal of this type in Canada – was drafted following an extensive consultation process conducted in 2002 by the federal departments of Justice, Industry and the Solicitor General. Representatives from police services, the telecommunications industry, civil society groups and individuals expressed their views on the issue.

Bill C-74 responded to a concern of law enforcement and national security agencies, who affirm that new technologies – such as Internet communications – often present obstacles to the lawful interception of communications. The bill's objectives were twofold:

---

(1) See Dominique Valiquet, *Telecommunications and Lawful Access: I. The Legislative Situation in Canada*, PRB 05-65E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 21 February 2006. That publication provides an overview of Bill C-74 and the consultations leading up to it.

(2) In the interests of conciseness, references in this text to "law enforcement agencies" include national security agencies, unless otherwise clearly indicated by the context.

(3) This technique, commonly called "wiretapping," is very useful for investigating a variety of crimes, in particular drug-related offences. For the precise number of convictions secured through the use of wiretaps, among other techniques, see Public Safety and Emergency Preparedness Canada, *Annual Report on the use of Electronic Surveillance – 2004*, Figures 3 and 4, http://www.psepc-sppcc.gc.ca/abt/dpr/le/elecsur-en.asp.

- To ensure that law enforcement agencies could legally intercept any communication, regardless of the technology used to send it;[4] this requirement would have compelled telecommunications service providers to have the technical capability to intercept communications made using their networks.

- To establish an expedited procedure enabling law enforcement agencies to identify a subscriber to a telecommunications service. Under this administrative procedure, the agencies could have accessed basic information about subscribers, without the need for a warrant or a judicial order. The bill did, however, establish certain protection measures.

At the time the bill was being developed, the debate on lawful access focussed primarily on privacy. The other important elements were the technical interception standards, the costs associated with an interception capability, and the need for new lawful access rules. The debate on these issues continues.

Bill C-74 was intended as a key step in the harmonization of legislation at the international level, specifically 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*.[5] The Department of Public Safety and Emergency Preparedness also justified its bill by referring specifically to the examples set by Australia and the United Kingdom.

The present document compares Bill C-74 with similar legislation in these three countries. Major differences and similarities are highlighted, with particular reference to the two aspects covered in the Canadian bill: interception capability, and requests for information about subscribers to telecommunications services. The comparison will provide useful information because the bill was the first legislative attempt to provide a framework for lawful access in Canada, it was the end product of an extensive consultation process, and many of its components may provide a basis for future legislative provisions in this regard.

---

(4) For instance, both Internet communications and communications using the traditional telephone system must be capable of interception.

(5) The Convention entered into force on 1 July 2004. However, many countries – for instance, Germany, Spain, the United Kingdom and the four non-member states of the Council of Europe which signed the Convention (South Africa, Canada, the United States and Japan) – have not yet ratified it. France ratified the Convention on 10 January 2006. The status of signatures and ratifications is presented on the Council of Europe Web site, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=10/01/2006&CL=FRE (consulted 26 January 2006).

UNITED STATES

The United States has one of the oldest and most frequently amended legislative schemes. The U.S. legislation has many flaws and certain historical incongruities. The many amendments are due in part to the fact that U.S. legislators had a specific type of technology in mind at the time when the scheme was originally implemented.(6)

A. Interception Capability

On 25 October 1994, in response to requests by the Federal Bureau of Investigation (FBI), the U.S. Congress enacted the Communications Assistance for Law Enforcement Act (CALEA).(7) The U.S. legislation deals only with the first aspect of Bill C-74, the communications interception capability imposed on telecommunications service providers. Like the Canadian bill, CALEA is not intended to broaden the investigative powers of law enforcement agencies. It is still necessary to have prior judicial authorization – or at least a court order or other lawful authorization – in order to intercept communications.(8)

The Federal Communications Commission (FCC) ruled that telecommunications carriers must be CALEA-compliant by 30 June 2002.(9) Today, the appropriate devices have been manufactured and are in use by telecommunications service providers. The FCC has, however, granted numerous exemptions, and CALEA's implementation is not yet complete.

1. Similar Provisions

CALEA contains a number of obligations that are similar to those set out in Bill C-74. In particular, telecommunications service providers must have the capability to:

- Intercept and isolate a communication (section 103; 47 USC 1002).

---

(6) Richard W. Downing, "Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime," *Columbia Journal of Transnational Law*, Vol. 43, No. 3, 2005, pp. 710, 717 and 718.

(7) P.L. 103-414, 47 USC 1001-1010.

(8) See section 105 of CALEA; 47 USC 1005. With regard to the wiretapping without court-approved warrants authorized by President George W. Bush for national security purposes and the fight against terror, see James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *The New York Times*, 16 December 2005, p. 1.

(9) The many disputes between law enforcement agencies, the telecommunications industry and privacy advocacy groups have caused delays in implementing the regulations. The disputes have focused primarily on technical standards, cost sharing and privacy protection. The debate is far from over.

- Simultaneously intercept communications of multiple users (section 104; 47 USC 1003).
- Isolate the transmission data[10] (section 103; 47 USC 1002).
- Provide the intercepted communication and the transmission data to law enforcement agencies (section 103; 47 USC 1002).
- Remove, where possible, any measures taken to protect a communication, such as encryption (section 103; 47 USC 1002).
- Ensure that all interceptions are kept confidential (section 103; 47 USC 1002).

In addition:

- The FCC may exempt a class of telecommunications service providers from compliance with the Act (section 102; 47 USC 1001).
- The obligations relating to interception capability do not apply to intermediary services or to private networks (section 103; 47 USC 1002).

2. Differences

a. Examples

There are also differences between Bill C-74 and CALEA.

- CALEA goes into greater depth about the expenses incurred by telecommunications service providers in order to comply with the legislation. The Attorney General may pay carriers for all reasonable costs (section 109; 47 USC 1008),[11] and a special fund has been set up for this purpose (section 110; 47 USC 1009).[12]

---

(10) Bill C-74 defined "transmission data" as follows: "data relating to the telecommunications functions of dialling, routing, addressing or signalling that identifies or purports to identify the origin, type, direction, date, time, duration, size, destination or termination of a telecommunication generated or received by means of a telecommunications facility or the type of telecommunications service used and includes any information that may be obtained under subsection 492.2(1) of the *Criminal Code* [number recorder]." While the definition is more or less the same throughout the world, it is important to note that the meaning of "transmission data" may very from one country to the next, such as in the United Kingdom.

(11) Unlike the system proposed by Bill C-74, this is a discretionary power. However, the U.S. Attorney General may cover expenses in all cases, while Bill C-74 would have required the Minister of Public Safety and Emergency Preparedness to pay reasonable costs only when he or she had issued an order.

(12) Section 110 of CALEA provides for an annual amount of $500 million for the period from 1995 to 1998. According to the telecommunications industry and the Justice Department Inspector General, the amount remaining will be insufficient (Patricia Moloney Figliola, *Digital Surveillance: The Communications Assistance for Law Enforcement Act*, Report for Congress, RL30677, Congressional Research Service, Library of Congress, 3 May 2005, pp. 10 and 13).

- CALEA states explicitly that the Attorney General will consult with the telecommunications industry in order to implement technical standards for interception (section 107; 47 USC 1006).

- CALEA states that if a telecommunications service provider uses devices that are in compliance with the standards put forward by the industry or an organization, it is to comply with the requirements on interception capability (section 107; 47 USC 1006).(13)

- A telecommunications service provider that does not comply with CALEA requirements is liable to a penalty of $10,000 per day (section 108; 18 USC 2522).

b. Internet Communications

Unlike Bill C-74, which applies to all technologies, CALEA was drafted initially to ensure that law enforcement agencies would be able to intercept telephone communications.(14) CALEA states that it does not apply to Internet service providers (ISPs).(15)

In view of the fears created by the terrorist attacks and pressure from the Bush administration,(16) the FCC issued an order in September 2005(17) that broadband ISPs and many of the companies providing Internet telephone services(18) would be governed by the CALEA requirements.(19) Compliance is required by April 2007.

---

(13) The so-called "Safe Harbor" provision. Based on this provision, the Telecommunications Industry Association, representing telecommunications equipment manufacturers, developed standard J-STD-025, also known as the "J-standard," which has been incorporated into telecommunications facilities. However, the FBI argued that the standard was not sufficiently inclusive and that it did not satisfy CALEA requirements. The FCC therefore required telecommunications service providers to add certain additional technical capabilities ("Punch List" items) to their networks before 30 June 2004. For example, the devices must be able to intercept digits dialled after the initial call set-up. Telecommunications service providers must also be able to link transmission data with the content of an intercepted communication (see FCC 99-230, Third Report and Order, CC Docket No. 97-213, 31 August 1999). This latter requirement was explicitly set out in Bill C-74.

(14) Declan McCullagh, "FBI Net-wiretapping rules face challenges," *CNet News.com*, 24 October 2005, http://news.com.com/FBI+Net-wiretapping+rules+face+challenges/2100-1028_35911676.html?tag=nefd.lede.

(15) Section 102 of CALEA; 47 USC 1001, the definitions of "information services" and telecommunications carrier"; section 103 of CALEA; 47 USC 1001. See also Committee on the Judiciary, Report, *Telecommunications Carrier Assistance to the Government*, House of Representatives, 103rd Congress, 2nd Session, 4 October 1994.

(16) Considering also the political context surrounding the renewal of the USA PATRIOT Act (P.L. 107-56, 111 Stat. 272 (2001)).

(17) FCC 05-153, First Report and Order, CC Docket No. 04-295, 23 September 2005.

(18) "Voice over Internet Protocol" (VoIP). Only systems interconnected with the public telephone system are affected (such as "Vonage" and "SkypeOut" services).

(19) Anne Broache, "Feds' Net-wiretap order set to kick in," *CNet News.com*, 11 November 2005, http://news.com.com/Feds+Net-wiretap+order+set+to+kick+in/2100-1028_3-5946880.html.

Although the order broadens CALEA's scope, it is silent on the situation of universities, research firms and small telecommunications service providers, which would have been excluded from the application of Bill C-74. It may therefore be assumed that a university or a small company providing Internet services through a modem cable, a digital subscriber line or a wireless network would be subject to CALEA's onerous requirement, and this is why a number of groups, including the American Council on Education, have taken legal action.(20)

B. Information About Subscribers

Like the scheme proposed in Bill C-74, certain designated persons in the government may, without a prior warrant or judicial order, compel a telecommunications service provider to give them information about its subscribers.(21)

In comparison with Canada's proposed system, more types of information are to be provided.(22) Furthermore, it appears that, under the U.S. system, more people are authorized to make an administrative order of this kind.(23)

UNITED KINGDOM

In July 2000, the United Kingdom enacted the *Regulation of Investigatory Powers Act* (RIPA),(24) in order to reflect technological change in the telecommunications industry. Like Bill C-74, RIPA applies to all current and future technologies.

---

(20) One of the arguments put forward was that it is not necessary to broaden CALEA in order to conduct Internet wiretaps – they were conducted long before the law was enacted. See Declan McCullagh, "Perspective: Net wiretapping plans under fire," *CNet News.com*, 19 December 2005, http://news.com.com/Net+wiretapping+plans+under+fire/2010-1071_3-5999138.html.

(21) 18 USC 2703(*c*)(1)(E) and (2). This is called an "administrative subpoena."

(22) In addition to the subscriber's name and address, telephone number and Internet Protocol (IP) address (items also covered in Bill C-74), the U.S. system also includes the date, time and length of the communication, along with the method of payment, bank information and credit card number.

(23) Hearing before the United States Senate Judiciary Committee, Subcommittee on Terrorism, Technology and Homeland Security, *Tools to Fight Terrorism: Subpoena Authority and Pretrial Detention of Terrorists*, Testimony of Rachel Brand, Principal Deputy Assistant Attorney General, Office of Legal Policy, U.S. Department of Justice, 22 June 2004, http://kyl.senate.gov/legis_center/subdocs/062204_brand.pdf.

(24) Chapter 23. It came into effect in October 2000, replacing the *Interception of Communications Act 1985*.

Its aim is to strike a balance between the powers of investigation held by law enforcement agencies and the protection of basic rights, especially privacy.(25) Communication interception warrants are issued by the Home Secretary(26) or, in emergency situations, by a senior government official.

A. Interception Capability

Sections 12-14 of RIPA concern the technical capability to intercept communications. This aspect of the draft legislation produced the greatest response from ISPs, specifically with regard to implementation costs.(27) The government's analysis of responses received during consultations stated that the requirements must not be too restrictive to ensure they do not constitute a major obstacle to trade. Furthermore, the Data Protection Commissioner stressed that the government should not place obligations on telecommunications service providers that might require them to jeopardize the privacy rights of their clients.(28)

1. Similar Provisions

RIPA contains some provisions that are similar to those provided in Bill C-74.

- Providers of public communication services may be required to maintain a reasonable interception capability (section 12).(29)
- An injunction may be issued to a public communications service provider that does not comply with the requirements (section 12(7)).

(25) See the ruling in *Halford* v. *United Kingdom*, 1997, European Court of Human Rights (73/1996/692/884).

(26) The exercise of this authority is subject to review by the Interception of Communications Commissioner.

(27) Gabrielle Garton Grimwood and Christopher Barclay, *The Regulation of Investigatory Powers Bill*, Research Paper 00/25, House of Commons Library, 3 March 2000, pp. 32 and 33.

(28) Trade and Industry Select Committee, *"Building Confidence in Electronic Commerce": The Government's Proposals*, HC 187 of 1998-1999, May 1999.

(29) The Home Secretary has the authority to impose such a requirement.

2. Differences

There are many differences between RIPA and Bill C-74. For example:

- RIPA governs postal services and telecommunications services (section 12(1)), whereas Bill C-74 would have applied only to telecommunications services.
- An order by the Home Secretary imposing interception capability must be presented to Parliament and approved by both Houses (section 12(10)).
- A public communications service provider may challenge the obligation to implement interception capability before a specialized advisory board (sections 12(5) and (6)).(30)
- The Home Secretary may in all cases pay the expenses of public communications service providers (section 14).
- A framework for encryption is established to ensure that a law enforcement organization in possession of a judicial authorization may compel *any person* to provide it with information in an intelligible form or to disclose the key to the protected information (sections 49(2) and 50(2)). The framework is much more detailed than the related scheme set out in Bill C-74, which would have applied only to telecommunications service providers.

B. Information About Subscribers

1. Storage of Transmission Data

The United Kingdom, unlike Canada, has a system that enables public communications service providers to collect and retain transmission data systematically.(31) There was no similar measure in Bill C-74.

Transmission data cover a wide range of information and may be retained for a specific period. For instance:

- Information about a subscriber(32) may be kept for 12 months.

---

(30) The Technical Advisory Board will examine the proposed technical standards and the financial impact on the provider's activities.

(31) *Anti-Terrorism Crime and Security Act 2001*, Ch. 24, Part 11; *Code of Practice for Voluntary Retention of Communication Data*. See Edgar A. Whitley and Ian Hosein, "Policy discourse and data retention: The technology politics of surveillance in the United Kingdom," *Telecommunications Policy*, Vol. 29, 2005. On 21 February 2006, the Council of the European Union adopted a directive on the retention of transmission data (Ireland and Slovakia voted against its adoption). Telecommunications service providers must now retain these data for a period from six months to two years. Following the directive's entry into force, member states will have 18 months in which to comply with its provisions (Reference: COD/2005/0182).

(32) Name, date of birth, telephone number, billing address, e-mail address, IP address, method of payment, credit card information, etc.

- Telephone information[33] may be kept for 12 months.
- Information about e-mails sent and received[34] may be kept for 6 months.
- Information about Internet activities[35] may be kept for 4 days.[36]

2. Comparison With the Request for Information Under Bill C-74

Sections 21-25 of RIPA establish a system enabling law enforcement agencies to have access to transmission data. This may be compared with the request for information on subscribers proposed in Bill C-74.

Similarities include the following:

- The request is submitted by a designated person and does not need to be pre-authorized by a judge (sections 22(4) and 25(2)).
- The request must be made primarily for the purposes of a criminal investigation, or in the interests of national security or public safety (section 22(2)).
- It must be possible to trace every request (section 23(1)).
- The legislation sets out protection measures. Under RIPA, an Interception of Communications Commissioner is appointed to review the exercise of the powers delegated to designated persons (section 57). Furthermore, a tribunal is responsible for hearing complaints from the general public (section 65 *et seq.*).[37]

On the other hand, there are significant differences in the nature of the information. The British system covers a great deal more information (transmission data)[38] than Bill C-74 (which covered only basic information identifying a subscriber, such as the name, address and telephone number). Other differences can be identified, for example:

---

(33) Telephone numbers, unique identifier, date, time and duration of the call, the location of the respondent, etc.

(34) IP addresses, e-mail addresses, date, time, etc.

(35) Date, time, IP addresses, URL addresses. The URL address retained contains only the domain name (e.g., http://www.parl.gc.ca). If there are characters after the domain name (for instance, http://www.parl.gc.ca/Search/Results.asp?lawful+access), they relate to content data and cannot therefore be retained systematically.

(36) Home Office, *Retention of Communications Data under Part 11: Anti-terrorism, Crime and Security Act 2001 – Voluntary Code of Practice*, Appendix 1.

(37) In addition to the Privacy Commissioner, Canada also has the Commission for Public Complaints against the RCMP (regarding RCMP activities), and the Security Intelligence Review Committee (regarding activities of the Canadian Security Intelligence Service).

(38) RIPA, section 21(4).

- RIPA states that the information requested must be proportionate to the purpose of the request (section 22(5)).
- The Home Secretary must provide financial compensation covering the expenses incurred by public communications service providers (section 24).

AUSTRALIA

The framework for Australia's system of lawful access is provided by two major laws: the *Telecommunications (interception) Act 1979* and the *Telecommunications Act 1997*. Both acts require that a warrant be issued before law enforcement agencies may access stored data or intercept private communications in real time.(39)

Australia has not signed the *Convention on Cybercrime*, unlike Canada, the United States and the United Kingdom.

A. Interception Capability

The requirements for interception capability are set out in the *Telecommunications Act 1997*. The Australian Communications and Media Authority (ACMA) is responsible for reviewing compliance with these requirements.

1. Similar Provisions

The *Telecommunications Act 1997* and Bill C-74 have certain similarities, including the following:

- Telecommunications service providers must comply with the requirements for interception capability (Part 15).
- Telecommunications service providers must provide assistance to law enforcement agencies, primarily in the execution of warrants and delivery of information (Parts 14 and 15).
- The process must remain confidential. No telecommunications service provider may disclose intercepted information, and users' privacy is protected by provisions governing transmission data, content data and personal information (Part 13).
- Exemptions may be granted (sections 325-327).(40)

(39) As in Canada, the issuance of a warrant for real-time interception is subject to more stringent regulations.

(40) The Minister of Communications and a special agency (the Agency Co-ordinator) have the authority to exempt a telecommunications service provider from interception capability obligations. ACMA may also grant an exemption to a provider that is implementing a trial service.

2. Differences

There are also certain differences between the Australian legislation and Bill C-74. For instance:

- Every telecommunications service provider must present an annual plan[41] setting out the measures to be taken to satisfy the requirements relating to interception capability (section 328 *et seq.*).[42]
- The maximum penalty in the event of non-compliance with the requirements is extremely high – $50,000 for an individual, and $10 million in the case of a company (sections 570(3) and (4)).[43]
- A telecommunications service provider must endeavour to prevent telecommunications networks and facilities from being used in, or in relation to, the commission of offences (section 313).
- There is provision for cost sharing between the telecommunications industry and law enforcement agencies. Telecommunications service providers pay most of the capital costs and ongoing costs of developing and maintaining an interception capability (section 332K *et seq.*). Law enforcement agencies pay costs incurred in the formatting and delivery of information. Details of the cost-sharing arrangements are set out in a contract between the provider and the law enforcement agencies.[44]
- The Act states that the implementation of an international technical standard fulfils the obligations relating to interception capability (section 322).
- The Act establishes an agency, called the Agency Co-ordinator, that is the point of contact between law enforcement agencies and the telecommunications industry on interception issues (section 7A). The Agency Co-ordinator is responsible for gathering comments from law enforcement agencies about providers' interception capability. The agency also offers legal advice on aspects of lawful access.

---

(41) Called the Interception Capability Plan.

(42) In 2004, some of the providers did not submit a plan. Their case was brought to ACMA's attention, but no charges were laid (Anthony S. Blunn, *Report of the review of the regulation of access to communications*, Government of Australia, Attorney-General's Department, August 2005, p. 40).

(43) See ACMA, *Telecommunications Interception Review – Review of the Longer Term Cost-Effectiveness of Telecommunications Interception Arrangements Under Section 332R of the Telecommunications Act 1997*, June 1999, p. 33. Bill C-74 proposed penalties of $100,000 in the case of an individual and $500,000 for a company.

(44) Blunn (2005), p. 49.

B. Information About Subscribers

The Australian legislation, like Bill C-74, allows law enforcement agencies to access subscriber information without having first obtained a warrant or a judicial order. However, the system in effect has a number of specific elements.

Unlike Bill C-74, the Australian scheme establishes a database(45) containing not only the subscriber's name, address, and telephone number, but also the location of the telephone device and whether the telephone is to be used for government, business, charitable or private purposes.(46)

Law enforcement agencies may access this database for national security reasons as well as for the purposes of enforcing the criminal law and safeguarding public revenue.(47) Although there is a Telecommunications Industry Ombudsman who can investigate complaints about telecommunications service providers, the protection measures proposed in Bill C-74 appear to be more comprehensive. Furthermore, it should be mentioned that Australia, unlike Canada, has regulations on storing transmission data.(48)

CONCLUSION

The *Convention on Cybercrime* calls for greater cooperation between countries and, consequently, harmonization of lawful access legislation. Bill C-74 was, of course, based on legislation existing in other countries, primarily the United States, the United Kingdom and Australia. Nevertheless, Canada's bill set out a particularly Canadian scheme. While the two central elements – interception capability and the administrative order – are also found in the U.S., British and Australian legislation, some details set the proposed Canadian legislation apart from the other systems.

---

(45) Called the "integrated public number database." See Part 4, Schedule 2, of the *Telecommunications Act 1997*.

(46) *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997*, section 10(4).

(47) *Ibid*., section 10(8).

(48) Downing (2005), p. 758.

With regard to interception capability, Bill C-74 was less ambiguous than the U.S. legislation, which is quite vague about the status of ISPs, universities and small telecommunications companies. The ambiguity can be attributed in part to the fact that the substantive rules were drafted by an administrative organization, the FCC.

It should be noted, however, that a similar situation might have arisen in Canada if certain elements of the system had been set out in regulations rather than pursuant to federal legislation. While it is true that legislation cannot provide for every eventuality, Bill C-74 did not provide a framework that was broad enough to predict future directions in the treatment of important issues such as cost sharing and technical interception standards. Should Canada follow in the footsteps of the United States by creating a special fund, of the United Kingdom by giving substantial discretionary authority to the government, or of Australia by requiring telecommunications service providers to pay almost all the costs inherent in ensuring interception capability? Should Canada also adopt an internationally recognized technical standard, or should we develop our own standards that suit our own purposes?

In terms of information about subscribers, the scheme set out in Bill C-74 appeared to be more restrictive than that of the other three countries. The types of information that a law enforcement agency would have been able to obtain without a warrant or a judicial order were more limited. The administrative order proposed in the bill would not have allowed the collection of much of the information covered by the other countries' legislation, specifically, the date, the time and the length of the communication, banking information, method of payment, credit card information (United States and United Kingdom) or the location of the telephone (United Kingdom and Australia). Finally, it should be noted that Bill C-74 did not call for a transmission data storage system, unlike the legislation in the United Kingdom and Australia.