Telecommunications and Lawful Access:
The Legislative Situation in the United States,
the United Kingdom and Australia

Publication No. 2005-66-E
28 February 2006
Revised 6 August 2012

Rebecca Katz
Dominique Valiquet
Legal and Legislative Affairs Division
Parliamentary Information and Research Service
Telecommunications and Lawful Access: The Legislative Situation in the United States, the United Kingdom and Australia
(Background Paper)

HTML and PDF versions of this publication are available on IntraParl (the parliamentary intranet) and on the Parliament of Canada website.

In the electronic versions, a number of the endnote entries contain hyperlinks to referenced resources.

Ce document est également publié en français.

Library of Parliament Background Papers provide in-depth studies of policy issues. They feature historical background, current information and references, and many anticipate the emergence of the issues they examine. They are prepared by the Parliamentary Information and Research Service, which carries out research for and provides information and analysis to parliamentarians and Senate and House of Commons committees and parliamentary associations in an objective, impartial manner.
1 INTRODUCTION

This paper deals with “lawful access,” an investigative technique used by law enforcement agencies and national security agencies. It involves the interception of communications and seizure of information during a search, where authorized by law.

During the first session of the 41st Parliament, in February 2012, the Minister of Public Safety introduced a bill on “wiretapping” in the era of new electronic technologies. Bill C-30, An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other acts (short title: Protecting Children from Internet Predators Act), revisits the subject matter of several former bills, including Bill C-50, Bill C-51 and Bill C-52, introduced in the third session of the 40th Parliament, and Bill C-74, introduced in the first session of the 38th Parliament.

Bill C-30 responds to the concerns of law enforcement and national security agencies that new technologies – such as Internet communications – often present obstacles to the lawful interception of communications. The bill has two parts, each responding to one of its central objectives.

- Part 1 creates the Investigating and Preventing Criminal Electronic Communications Act, a new law governing telecommunications service providers (TSPs).
- Part 2 amends the Criminal Code and several other acts in order to modernize investigative and interception techniques available to law enforcement and in order to modernize certain offences.

As well, Bill C-12, introduced several months before Bill C-30, amends the Personal Information Protection and Electronic Documents Act to expand the circumstances in which law enforcement agencies can ask private organizations to disclose personal information without the consent of the individual concerned.

The legislative debate on Bill C-30 and its predecessors has largely focused on privacy. Other important considerations include a new requirement that TSPs (including Internet service providers) put in place interception capabilities, the technical standards for and costs of these capabilities, and the need for new lawful access rules. The debate on these issues continues.

In addition to responding to the concerns of Canadian law enforcement authorities, Bill C-30 represents a step towards harmonizing the methods available to counter cybercrime internationally. Canada signed the Council of Europe’s Convention on Cybercrime in 2001 and the Additional Protocol concerning acts of a racist or
xenophobic nature committed through computer systems in 2005. The Convention requires that member states adopt legal methods to curtail criminal activity that uses new technologies and criminalize certain uses of computer systems. Bill C-30, like some of its predecessors, would allow Canada to ratify the Convention and Protocol. Its provisions also resemble requirements found in the legislation of several other countries, such as the United States, the United Kingdom and Australia. Both the United States and United Kingdom have ratified the Convention, in 2006 and 2011, respectively, whereas Australia has not yet signed it.5

This background paper compares Bill C-30 with similar legislation in these three countries. Major differences and similarities are highlighted, with particular reference to three aspects covered in the Canadian bill: interception capability, requests to TSPs for information about subscribers and tracking warrants. The comparison is a useful one because Bill C-30 is the latest of several significant Canadian initiatives that have dealt with lawful access and that have proposed consistently similar provisions.

2 UNITED STATES

The United States has one of the oldest and most frequently amended legislative schemes. 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 As a result, the U.S. legislation has many flaws and some historical incongruities.

2.1 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 with only one aspect of Bill C-30: the communications interception capability imposed on TSPs. 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 – 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 spring 2007.9 Today, the appropriate devices have been manufactured and are in use by TSPs. The FCC has, however, granted numerous exemptions, and CALEA’s implementation is not yet complete.

2.1.1 SIMILAR PROVISIONS

At present, no Canadian legislation compels all TSPs to use apparatus capable of intercepting communications. Only licensees that use radio frequencies for wireless voice telephone services have been required, since 1996, to have equipment permitting such interceptions.
As in the United States, to intercept the content of private communications, Canadian law enforcement agencies and the Canadian Security Intelligence Service (CSIS) generally require prior legal authorization, usually in the form of a judicial warrant. Bill C-30 does not alter these requirements. Similar to CALEA, Bill C-30 requires all TSPs to possess the technical capacity to allow law enforcement and national security agencies to intercept communications sent via the TSP, once the relevant legal authorization has been obtained.

CALEA contains a number of obligations similar to those set out in Bill C-30. In particular, TSPs must have the capability to:

- intercept and isolate a communication;
- simultaneously intercept communications of multiple users;
- isolate transmission data;
- provide the intercepted communication and transmission data to law enforcement agencies;
- remove, where possible, any measures taken to protect a communication, such as encryption; and
- ensure that all interceptions are kept confidential.

In addition:

- the FCC may exempt a class of TSPs from compliance with the Act, and
- the obligations relating to interception capability do not apply to intermediary services or to private networks.

2.1.2 DIFFERENCES

2.1.2.1 EXAMPLES

There are also differences between Bill C-30 and CALEA.

- CALEA goes into greater depth about the expenses incurred by TSPs in order to comply with the legislation. The Attorney General may pay carriers for all reasonable costs, and a special fund has been set up for this purpose.
- CALEA states explicitly that the Attorney General will consult with the telecommunications industry in order to implement technical standards for interception.
- CALEA states that if a TSP uses devices that comply with the standards put forward by the industry or an organization, it must comply with the requirements on interception capability.
2.1.2.2 INTERNET COMMUNICATIONS

Unlike Bill C-30, which applies to all technologies, CALEA was drafted initially to ensure that law enforcement agencies would be able to intercept telephone communications.\(^{18}\) CALEA states that it does not apply to Internet service providers (ISPs).\(^{19}\)

However, because of fears of terrorist attacks and pressure from the Bush administration,\(^{20}\) the FCC issued an order in September 2005\(^{21}\) that broadband ISPs and many of the companies providing Internet telephone services\(^{22}\) would be governed by the CALEA requirements.\(^{23}\) Compliance was required by April 2007.

Although the order broadens CALEA’s scope, it is silent on the situation of universities, research firms and small telecommunications service providers. A university or a small company providing Internet services through a modem cable, a digital subscriber line or a wireless network may therefore be subject to CALEA’s onerous requirement. Because of concern about this possibility, a number of groups, including the American Council on Education, have taken legal action.\(^{24}\) By contrast, these service providers are clearly excluded from the application of Bill C-30 in Canada.

2.2 INFORMATION ABOUT SUBSCRIBERS

At present in Canada, in most circumstances, private organizations must disclose personal information about clients to law enforcement and national security agencies without the consent of the individual concerned, if the relevant agency has judicial or other legal authorization to compel the production of the information. Without a warrant, the disclosure of personal information is not mandatory. However, TSPs in Canada may disclose clients’ personal information to law enforcement agencies voluntarily in circumstances permitted under their subscriber agreements, although they generally do so only in case of imminent danger to life or property.

The legality of police requests for voluntary disclosure of subscriber information by TSPs (in the absence of a warrant) has been challenged before the courts as a violation of the right to privacy under the *Canadian Charter of Rights and Freedoms*. The Supreme Court of Canada has held that individuals have a reasonable expectation of privacy concerning information that tends to reveal intimate details about their lifestyle and personal choices. However, the cases relating to subscriber information have been very context-specific, and the exact circumstances in which individuals have a reasonable expectation of privacy in relation to this information remain unclear. Nonetheless, recent case law suggests that the more that subscriber information tends to reveal patterns of use that could expose intimate details about lifestyle or personality, the greater the likelihood that individuals would have a reasonable expectation of privacy concerning that information.\(^{25}\)

Bill C-30 aims to clarify the types of information associated with subscriber services and equipment that may be disclosed to law enforcement or national security...
agencies without a warrant for investigative purposes, by specifically including the following: name, address, telephone number, email address, Internet protocol (IP) address and local service provider identifier. Accessing other information will continue to require a warrant.

In the United States, like the scheme proposed in Bill C-30, certain designated persons in the government may, without a prior warrant or judicial order, compel a TSP to give them information about its subscribers.26

In contrast to Canada’s proposed system, more types of information may be provided in the United States.27 Furthermore, under the U.S. system, it appears that more people are authorized to make an administrative order of this kind.28

2.3 TRACKING WARRANTS

Currently in Canada, section 492.1 of the Criminal Code allows a peace officer with a warrant – although a warrant is not necessary in urgent situations – to secretly install a “tracking device” (that is, a device that may be used to record or transmit tracking data in real time; e.g., a global positioning system [GPS] device) on a thing (explained below), if the officer suspects that an offence has been or will be committed and information obtained through such a tracking device, notably the location of a person, would assist in the investigation.

Bill C-30 retains this type of warrant but makes a distinction, in terms of the standard of proof required, between a warrant to install a tracking device on a thing, such as a vehicle, to track its movements, and a warrant to install that kind of device on a thing usually carried or worn by an individual, such as a cellular telephone, to track the individual’s location and movements.

Under Bill C-30, the test for granting a warrant to track the movements of a thing is based on the existing standard, reasonable grounds to suspect that an offence has been or will be committed, while a more stringent standard applies to a warrant to track the movements of an individual: reasonable grounds to believe that an offence has been or will be committed. In addition to allowing a tracking device to be installed, which is already permitted if a judicial order is obtained, the bill allows law enforcement agencies to remotely activate devices of that kind that are found in certain types of technology, such as cellular telephones or the GPS devices in certain cars.

With regard to the other type of tracking warrant proposed by Bill C-30, section 492.2(1) of the Criminal Code allows a peace officer with a warrant to secretly install a number recorder on a telephone or telephone line if the officer suspects that an offence has been or will be committed and if information obtained through this kind of recorder would assist in the investigation. The law enforcement agency could thus obtain the incoming and outgoing telephone numbers for a telephone that was being tapped.

Bill C-30 also provides for a warrant authorizing a peace officer to install and activate a traffic data recorder, which provides data on the origin and destination of an
Internet communication, for example. Police services would thus have access to this traffic data in real time. Like a warrant to install a telephone number recorder, the new warrant will be based on the requirement of reasonable grounds to suspect that an offence has been or will be committed.

In the United States, a court order for a pen register (to obtain telephone numbers) or a trap-and-trace device (to obtain location or traffic data) can be obtained by law enforcement agencies under a even lower threshold than in Canada: that the information likely to be obtained is relevant to an ongoing criminal investigation.

Amendments made by the Patriot Act went further by creating “roving orders.” Rather than obtaining a separate court order for every telephone or device they wish to tap, intelligence officers can obtain a global order allowing them to tap multiple devices belonging to a single individual. In other words, these orders allow them to target a person, rather than a specific phone or device. Bill C-30 does not seem to address the issue of roving orders. However, it allows a judge to authorize interception of communications and, at the same time, issue related warrants, such as those for search and tracking.

3 UNITED KINGDOM

In July 2000, the United Kingdom enacted the Regulation of Investigatory Powers Act (RIPA) in order to reflect technological change in the telecommunications industry. Like Bill C-30, RIPA applies to all current and future technologies.

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. Communication interception warrants are issued by the Secretary of State for the Home Department (the “Home Secretary,” the Cabinet minister responsible for internal affairs) or, in emergency situations, by a senior government official.

3.1 INTERCEPTION CAPABILITY

Sections 12–14 of RIPA concern the technical capability to intercept communications. In its initial draft, this aspect of RIPA produced the greatest response from TSPs, specifically with regard to implementation costs. 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 TPSs that might require them to jeopardize the privacy rights of their clients.
3.1.1 Similar Provisions

RIPA contains some provisions similar to those provided in Bill C-30.

- Providers of public communication services may be required to maintain a reasonable interception capability.\(^{37}\)
- An order may be issued to a public communications service provider that does not comply with the requirements.\(^{38}\)

3.1.2 Differences

There are many differences between RIPA and Bill C-30. For example:

- RIPA governs postal services and telecommunications services, whereas Bill C-30's provisions deal only with telecommunications services;
- An order by the Home Secretary imposing interception capability must be presented to Parliament and approved by both Houses;
- A public communications service provider may challenge the obligation to implement interception capability before a specialized advisory board;\(^{39}\)
- The Home Secretary may in all cases pay the expenses of public communications service providers;\(^{40}\)
- RIPA establishes a framework for encrypted communications to ensure that a law enforcement agency with 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.\(^{41}\)

The framework established in the legislation is more detailed than the related scheme set out in Bill C-30, which requires TSPs to provide decrypted communications only if they have the technical capacity to do so and does not require them to implement such capacity.

3.2 Information about Subscribers

3.2.1 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.\(^{42}\) There is no similar measure in Bill C-30.

Transmission data may also be referred to as “communications data” in the United Kingdom. The terms cover a wide range of information, which may be retained for specific periods under British legislation. For instance,

- information about a subscriber\(^{43}\) may be kept for 12 months;
- telephone information\(^{44}\) may be kept for 12 months;
• information about email messages sent and received\textsuperscript{45} may be kept for six months; and
• information about Internet activities\textsuperscript{46} may be kept for four days.\textsuperscript{47}

3.2.2 Comparison with the Request for Information Under Bill C-30

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-30.

Similarities include the following:

• The request is submitted by a designated person and does not need to be authorized by a judge.\textsuperscript{48}
• It must be possible to trace records of every request.\textsuperscript{49}

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)\textsuperscript{50} than Bill C-30 (which covers only information identifying a subscriber, such as name, address and telephone number). Other differences include the following:

• RIPA states that the information requested must be proportionate to the purpose of the request, and such purposes seem to be broader than what is allowed under Bill C-30.\textsuperscript{51}
• The legislation sets out more specific protection measures. Under RIPA, an Interception of Communications Commissioner is appointed to review the exercise of the powers delegated to designated persons. Furthermore, a tribunal is responsible for hearing complaints from the general public.\textsuperscript{52}

3.2.3 Proposed Changes

In June 2012, the Home Secretary presented a draft Communications Data Bill to the U.K. Parliament.\textsuperscript{53} The Secretary noted that the draft bill is to be reviewed by a Joint Committee of Parliament as well as by the Intelligence and Security Committee before being introduced in Parliament later in the session.\textsuperscript{54} The draft bill proposes to amend lawful access legislation in the United Kingdom in several ways. Notably, it would

• amend the framework for compiling “traffic, use and subscriber data”\textsuperscript{55} to ensure that telecommunications and postal services operators make available a broader range of data to public authorities, including some data that service providers would not ordinarily generate for business reasons;
• update the scheme for relevant public authorities to obtain communications data and establish procedures for dedicated senior officers to access data, subject to tests of necessity and proportionality;
• confer additional scrutiny functions on the Interception of Communications Commissioner and the Investigatory Powers Tribunal; and
• establish procedures to make orders and to arrange financial compensation to service providers for costs incurred in complying with the legislation.

Like the current legislative scheme, the draft bill would apply to postal services as well as TSPs. The draft bill would not change the requirement to obtain judicial authorization to access communications content; it only enables access to “traffic, use and subscriber data”, which would not require the authorization of a magistrate in the case of requests made by police and other public authorities.56

3.3 TRACKING WARRANTS

In the United Kingdom, the Home Secretary and other designated persons have the power to authorize the use of surveillance devices for broader purposes than those permitted by Canadian legislation. In both Canada and the United Kingdom, preventing and detecting crime are considered legitimate purposes. As well, in the United Kingdom, assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department is another recognized purpose.57

However, the U.K. legislation includes an additional requirement not expressly found in Bill C-30: “that the authorised surveillance is proportionate to what is sought to be achieved by carrying it out (‘the balancing test’).”58

4 AUSTRALIA

The framework for Australia’s system of lawful access is provided by two major laws: the Telecommunications (Interception and Access) 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.59

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

4.1 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.
4.1.1 Similar Provisions

The Telecommunications Act 1997 and Bill C-30 have certain similarities, including the following:

- TSPs must comply with the requirements for interception capability.
- TSPs must provide assistance to law enforcement agencies, primarily in the execution of warrants and delivery of information.
- The process must remain confidential. No TSP may disclose intercepted information, and users’ privacy is protected by provisions governing transmission data, content data and personal information.
- Exemptions may be granted.60

4.1.2 Differences

There are also certain differences between the Australian legislation and Bill C-30.

- Every TSP must present an annual plan61 of the measures to satisfy the requirements for interception capability.62
- The maximum penalty for non-compliance with the requirements is extremely high – $50,000 for an individual and $10 million for a company.63
- A TSP must endeavour to prevent telecommunications networks and facilities from being used in, or in relation to, the commission of offences.64 TSPs could therefore, in most cases, be viewed as “agents of the State.” While Bill C-30 does not contain the same requirement, TSPs in Canada could also be seen as agents of the state since the passage of the Act Respecting the Mandatory Reporting of Internet Child Pornography by Persons who Provide an Internet Service in March 2011.65
- There is provision for cost sharing between the telecommunications industry and law enforcement agencies. TSPs pay most of the capital and ongoing costs of developing and maintaining an interception capability. However, 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.66
- The Act states that the implementation of an international technical standard fulfils the interception capability obligations.67
- 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.68 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.
4.2 INFORMATION ABOUT SUBSCRIBERS

The Australian legislation, like Bill C-30, 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-30, the Australian scheme establishes a database containing not only the subscriber’s name, address and telephone number, but also the location of the telephone device and whether it is used for government, business, charitable or private purposes.

Law enforcement agencies may access this database for national security reasons as well as for enforcing the criminal law and safeguarding public revenue. Although there is a Telecommunications Industry Ombudsman who can investigate complaints about TSPs, the protection measures proposed in Bill C-30 appear to be more comprehensive. Furthermore, the Australian government is seeking to introduce mandatory data retention, a system forcing TSPs to collect and retain traffic data systematically. No such requirement is expressly proposed by Bill C-30.

4.3 TRACKING WARRANTS

Sections 14–21 of the Australian Surveillance Devices Act 2004 permit court orders to obtain phone numbers, location data and traffic data under a threshold similar to that proposed in Bill C-30 (suspicion based on reasonable grounds). However, generally speaking, these warrants can be obtained only for serious offences (punishable by a maximum term of three years’ imprisonment or more). No such limitation is found in Bill C-30. Furthermore, the Australian legislation provides for the presentation of annual reports on the use of these types of warrants before each House of Parliament. Bill C-30 has no such requirement.

The cybercrime legislation amendment bill 2011 would allow Australian agencies to obtain and disclose traffic data for the purposes of a foreign investigation. Bill C-30 includes a similar provision by amending the Mutual Legal Assistance in Criminal Matters Act.

5 CONCLUSION

The Convention on Cybercrime calls for greater cooperation among countries and, consequently, harmonization of lawful access legislation. Bill C-30 is based on legislation 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.
With regard to interception capability, Bill C-30 is 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 in the legislation. While legislation cannot provide for every eventuality, Bill C-30 does not provide a framework broad enough to predict future directions in 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 TSPs to pay almost all the costs inherent in ensuring interception capability?

In terms of information about subscribers, the scheme set out in Bill C-30 appears to be more restrictive than that of the other three countries. The types of information that a law enforcement agency can obtain without a warrant or a judicial authorization are more limited. The administrative order proposed in the bill will not allow the collection of much of the information covered by the other countries’ legislation; specifically, the date, the time and the length of the communication, instrument numbers, banking information, method of payment, credit card information (United States and United Kingdom) or the location of the telephone (United Kingdom and Australia). Finally, Bill C-30 does not establish a transmission data storage system, unlike the situation in the United Kingdom and Australia.

NOTES


2. Law enforcement agencies (police forces) and national security agencies (such as the CSIS and the Communications Security Establishment) may have differing powers and levels of judicial and administrative supervision. In the interests of conciseness, references in this background paper 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, Cat. No: PS1-1/2004E-PDF, Minister of Public Safety and Emergency Preparedness, Ottawa, 2005, Figures 3 and 4.

4. The Convention entered into force on 1 July 2004. However, some countries – such as South Africa and Canada – have not yet ratified it. The status of signatures and ratifications is presented at “Convention on Cybercrime – CETS No.: 185,” Council of Europe Treaty Office.
5. A bill that would probably allow Australia to ratify the Convention was given assent 12 September 2012; see Parliament of Australia, Cybercrime Legislation Amendment Bill.


9. The many disputes among 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.

10. The Communications Security Establishment, which is responsible for foreign intelligence collection, is shielded from criminal liability if it intercepts private communications incidental to its main intelligence functions.

11. According to the European Telecommunications Standards Institute (ETSI), “possessing the technical capability” means that the service provider must furnish an interface that enables preserved data to be delivered to a law enforcement agency in a reliable, secure, rapid and standardized fashion, with minimal disruption and cost to the provider. Canada helped draft ETSI’s technical specifications for lawful interception.

12. Subsection 2(1) of Bill C-30 defines “telecommunications data” as data that 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 that identify the type of telecommunications service used. The bill also includes “transmission data,” which applies to part 2. The Convention on Cybercrime uses a different term, “traffic data.” While these definitions are more or less the same throughout the world, the meaning of “transmission data” may vary from one country to another.

13. CALEA, 47 USC 1002, Title I, ss. 103 and 104.

14. Ibid., 47 USC 1001, Title I, ss. 102 and 103.

15. Unlike the system proposed by Bill C-30, this is a discretionary power. However, the U.S. Attorney General may cover expenses in all cases, while Bill C-30 provides for specific situations in which a law enforcement or national security agency must compensate a TSP (see Erin Shaw and Dominique Valiquet, Legislative Summary of Bill C-30: An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts, Publication no. 41-1-C30-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 15 February 2012, section 2.1.6).

17. CALEA, 47 USC 1006, Title I, s. 107. 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 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. 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 is explicitly set out in Bill C-30.


19. CALEA, 47 USC 1001, Title I, s. 102, the definitions of “information services” and “telecommunications carrier”; and s. 103. See also Committee on the Judiciary, Telecommunications Carrier Assistance to the Government, House of Representatives, 103rd Congress, 2nd Session, 4 October 1994.


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


24. 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.


26. 18 USC 2703(c)(1)(E) and (2). This is called an “administrative subpoena.”

27. In addition to the subscriber’s name and address, telephone number and Internet Protocol (IP) address (items also covered in Bill C-30), the U.S. system also includes the date, time and length of the communication, telephone records, instrument numbers, along with the method of payment, bank information and credit card number.

29. This includes Voice over Internet Protocol (VoIP), such as Skype and FaceTime.
30. 18 USC Chapter 206.
31. 50 USC Chapter 36.
34. The exercise of this authority is subject to review by the Interception of Communications Commissioner.
37. The Home Secretary has the authority to impose such a requirement.
38. RIPA, ss. 12 and 12(7).
39. Ibid., ss. 12(1), 12(10), 12(5) and 12(6). The Technical Advisory Board will examine the proposed technical standards and the financial impact on the provider’s activities.
40. Ibid., s. 14.
41. Ibid., ss. 49(2) and 50(2).
42. Anti-Terrorism Crime and Security Act 2001, c. 24, part 11: Retention of Communications 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). TSPs must now retain these data for a period from six months to two years. Following the directive’s entry into force, member states have 18 months in which to comply with its provisions. See European Parliament, Electronic Communications: Personal Data Protection Rules and Availability of Traffic Data for Anti-terrorism Purposes, 2005-0182(COD).
43. Name, date of birth, telephone number, billing address, email address, IP address, method of payment, credit card information, etc.
44. Telephone number; unique identifier; date, time and duration of the call; the location of the respondent; etc.
45. IP addresses, email addresses, date, time, etc.
46. 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.
48. RIPA, ss. 22(4) and 25(2).
49. Ibid., s. 23(1).
50. Ibid., s. 21(4).
51. Ibid., ss. 22(5) and 22(2). Under Bill C-30, designated members of police services may request, in writing, information that relates to any police function, whether it concerns the enforcement of federal or provincial laws or the laws of a foreign state. Individuals designated by CSIS and the Commissioner of Competition may request only information relating to their functions under their relevant enabling legislation. In the United Kingdom, transmission data can be requested on additional grounds, such as the interests of the economic well-being of the United Kingdom, the protection of public health or the collection of any tax, duty, levy or other imposition.

52. Ibid., ss. 57 and 65 and following. 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 CSIS).


54. Ibid., Foreword, p. i.

55. Ibid., see the definitions of traffic, use and subscriber data in section 28 of the bill.

56. Ibid., ss. 9 and 11.

57. RIPA, Part II.

58. Ibid., ss. 28(2) and 32(2).

59. As in Canada, issuing a warrant for real-time interception is subject to more stringent regulations.

60. Telecommunications Act 1997, Parts 13–15 and ss. 325–327. The Minister of Communications and a special agency (the Agency Co-ordinator) have the authority to exempt a TSP from interception capability obligations. ACMA may also grant an exemption to a provider that is implementing a trial service.

61. Called the Interception Capability Plan.

62. Telecommunications Act 1997, s. 328 and following. In 2004, some of the providers did not submit a plan. Their case was brought to ACMA’s attention, but no charges were laid. See 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.


64. Telecommunications Act 1997, s. 313.

65. For more information on Bill C-22, see Dominique Valiquet, Legislative Summary of Bill C-22: An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service, Publication no. 40-3-C22-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 15 February 2011.


67. Ibid., s. 322.

68. Ibid., s. 7A.

69. Called the "integrated public number database." See ibid., Part 4, Schedule 2.

70. Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997, s. 10(4).

71. Ibid., s. 10(8).
72. See the definition of “relevant offences.”

73. For more information about the bill, see Joint Select Committee on Cyber-safety, Review of the Cybercrime Legislation Amendment Bill 2011, Parliament of the Commonwealth of Australia, Canberra, August 2011.

74. As signatories to the Cybercrime Convention, the United States and the United Kingdom have similar provisions in their legislation.