Filing Information
August 2002
IDC #CA050TLJ
Volume: 1
Tab: Other

Canadian Telecom Market Drivers and Strategies

Bulletin

Caught in the Web: Ottawa's Implementation of Cyber-crime Treaty Requires Online Surveillance by xSPs

Analysts: Lawrence Surtees and Warren Chaisatien

IDC Opinion

The federal government announced a proposal on Aug. 25 to implement the Council of Europe's *Cyber-crime Convention* into Canadian law. We analyze those proposed legal changes and the impacts associated with:

- Requiring all telecommunications and Internet service providers to build automatic real-time surveillance capabilities into all of their networks to better enable national security and police agencies to spy on their customers' Web and e-mail activities;
- Creating a national database of all Internet users;
- Imposing financial burdens on service providers;
- Weakening privacy - and the position of industry players and privacy and civil liberties groups; and

- Broadening interception requirements through proposed EU traffic data retention measures.

> A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning.
>
> **- Mr. Justice Gerard V. La Forest, *Duarte v. The Queen* [1990]**

In this Study

The federal government's discussion paper on proposed changes to expand powers to intercept electronic communications is analyzed. The rationale for both Ottawa's 'Lawful Access' proposals and the European Union's *Cyber-crime Convention*, as well as the impact on telecommunication and Internet service providers is discussed. We examine U.S.-based lawful intercept programs and technical standards to provide insights into how Canadian service providers may implement mandatory intercept capabilities in their networks.

Controversial EU proposals for the mandatory retention of traffic data of all network users are also analyzed.

The views of leading privacy advocates, legal experts and major Canadian telecom and Internet service providers are discussed. We also provide guidance on the issues and questions that each service provider may wish to consider in their response to Ottawa.

Situation Overview

Justice Releases Controversial Discussion Paper

The federal government has begun a controversial process to harmonize Canadian laws on the interception of electronic communications with a proposed European Council Treaty on Cyber-Crime. The Department of Justice, the Solicitor-General and Industry Canada released a 21-page paper on Sunday, August 25, 2002 seeking comment from industry players and input from the public, as well as legal representatives, before legislation is drafted, likely by the end of this year or early in 2003. (See: Department of Justice, Industry Canada and Solicitor-General. *Lawful Access – Consultation Document,*

Ottawa: August 25, 2002. Available at: http://canada.justice.gc.ca/en/cons/la_al.)

At issue is Ottawa's desire to modernize its existing laws that already allow for communications interception, notably in the areas of real-time tracing of traffic data and interception of e-mail messages. The document also calls for Internet service providers (ISPs) to allow, "at a minimum," intercept capability when offering new services or upgraded service. It also proposes establishing a national database of Internet users.

"Legislation governing lawful access was originally designed for rotary telephones - not e-mail or the Internet," stated former Solicitor-General Lawrence MacAulay.[1] He made the comment in a speech launching the consultation process at the annual meeting of the Canadian Association of Chiefs of Police.

The Department of Justice discussion paper states the proposals address requirements stemming from three primary needs:

(1) The need to bring the provisions of the law into concordance with new telecommunications technology;

(2) A need for all telecommunications service providers to ensure that the technical capability in their facilities permits lawful access by law enforcement and national security agencies; and

(3) The need for Canada to adopt statutory measures that will permit ratification of the Council of Europe's *Convention on Cyber-Crime*.

Ottawa's existing intercept powers

The federal government already has significant powers to intercept communications - a well-established technique euphemistically termed "lawful access"- used by law enforcement and national security agencies to conduct investigations. The constitutionality of communication interception was first declared by the United States Supreme Court in 1928. In Canada, the Royal Canadian Mounted Police began using intercepts as an investigative technique in 1936.

Canadian law enforcement and national security agencies currently have powers to conduct electronic surveillance[2] – including interception of telecommunications and to search and seize information - pursuant to legal authority as provided in the

---

[1] Canada. *News Release*, August 25, 2002.

[2] Electronic surveillance is defined by intelligence agencies as: the "acquisition of a non-public communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non-electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction finding equipment solely to determine the location of a transmitter."

Criminal Code, the *Canadian Security Intelligence Service Act*, and other Acts of Parliament including the *Competition Act* and the *National Defence Act.*

Types of Interception

The requirements giving police the means to obtain judicial authorizations for electronic surveillance under section 185 and a warrant under section 487.01 are described in Parts VI and XV of the *Criminal Code*. [Comparable communications intercepts in the United States are obtained under Title III of the *Omnibus Crime Control and Safe Streets Act.*]

Communications interception for investigation of domestic national security threats in Canada is conducted by the Canadian Security Intelligence Service (CSIS). Under section 21 of the *CSIS Act*, only judges of the Federal Court of Canada have the power to issue intercept warrants. CSIS intercept warrants are also reviewed annually by the Security Intelligence Review Committee. SIRC's audits cover warrants, surveillance, targeting authorizations, community interviews and other matters. [In the United States, those intercepts are performed under the *Foreign Intelligence Surveillance Act* of 1978, with warrants issued by a select panel of 11 federal judges.][3]

Three types of communication interception are conducted:

- **Full content of conversations**. This involves call identifying and call content of calls placed or received by the intercept subject. Law enforcement agencies require the ability to distinguish between sounds spoken by the subject or heard by the subject.
- **Pen register**. Also termed dial number recorders (or DNRs), this device captures *outbound* call-identifying information (not call content) of parties whom the subject is calling; and
- **Trap and trace.** This type of intercept captures *inbound* call-identifying information (not call content) of parties the target is calling.

Legal experts believe the frequency of electronic surveillance use by law enforcement agencies in Canada for the investigation of domestic crime is widespread. Canadian authorities were prone to request 20 times more authorizations to conduct electronic surveillance than their U.S. counterparts, the Law Reform Commission of Canada stated in a 1990 report.[4]

---

[3] U.S. *Foreign Intelligence Surveillance Act (FISA)*, 50 U.S.C. §1801 et seq., Public Law No. 95-511.

[4] Canada. Law Reform Commission. *Electronic Surveillance*, Working Paper No. 47, Ottawa: 1986, p. 10; cited in: Supreme Court of Canada. *Duarte v. R.* [1990], p. 5.

The number of court warrants for telephone taps has also risen dramatically in Australia. Authorities requested 2,157 intercept warrants in fiscal 2000 - an almost 10-fold increase over the past decade, according to the latest government report.[5] (Table 1 on the following page compares the number of communications intercept warrants issued to law enforcement agencies in Australia, Canada, the United Kingdom and the United States in the past five years.)

Table 1

Telecommunications Intercept Warrants: Australia, Canada, United States and United Kingdom, 1995-2000

	FY1995	FY1996	FY1997	FY1998	FY1999	FY2000
Australia *TIA* intercepts				1284	1689	2157
Canada – Part VI *Criminal Code*	998	693	1420	737	736	
Canada - New *CSIS* s. 21 warrants	32	125	72	84	76	56
CSIS Warrants renewed	180	163	153	163	181	150
U.K. Wiretaps	1,046	1,301	1,647	1,913	1,734	NA
U.S. *Title III* call content intercepts	1,058	1,149	1,186	1,329	1,350	1,190
U.S. *FISA* intercepts						1,012

Note: Data excludes DNR and trap-and-trace intercepts. Sources: Australia. Attorney-General. *Telecommunications Interception Act Report for the year ending 30 June 2001*. Canada. Security Intelligence Review Committee. *SIRC Report 2000-2001;* Solicitor-General Canada. *Annual Report on the Use of Electronic Surveillance 1999*; United Kingdom. Home Office. *Annual report of the Interception of Communications Commissioner 1999*; United States. Administrative Office of the U.S. Courts; IDC Canada, 2002

Yet, the number of warrants issued alone does not provide a full picture of the scope of electronic surveillance activities. Statistics on the average number of conversations intercepted per wiretap and the number of persons intercepted per wiretap give a truer picture. For example, U.S. statistics for 2000 reveal that an average of 1,769 conversations made by 196 people were intercepted with each Title III warrant. More than 2.1 million conversations were monitored under those warrants.[6]

Data submitted by some telephone service providers in response to a U.S. congressional inquiry in 1993 also show that

---

[5] Australia. Attorney-General. *Telecommunications Interception Act Report for the year ending 30 June 2001*, Canberra: September 2002.

[6] Center for Democracy & Technology, "The Nature and Scope of Governmental Electronic Surveillance Activity," May 8, 2001.

additional customers are impacted by requests for records. Bell Atlantic (now **Verizon**), for example, indicated that for the years 1989 through 1992, it had responded to 25,453 subpoenas or court orders for toll billing records of 213,821 of its customers. NYNEX (also now a unit of Verizon) reported that it had processed 25,510 subpoenas covering an unrecorded number of customers in 1992 alone.[7] Australian police also resorted to 733,000 inspections of subscriber bills, including inward and outward calls, SMS messages, and the location of mobile phone calls, between June, 2000 to June, 2001.[8]

Australia

The volume of intercepts also rises dramatically when the number of pen register (DNR) and trap-and-trace wiretaps are included. IDC estimates there were 68,000 DNR and trap-and-trace intercepts conducted in the United States alone in 2000.[9]

War on terrorism expands scope of interception

Legislative changes enacted in many countries in the wake of Sept. 11 have also greatly expanded the authority of law enforcement and national security agencies to intercept communications.

The scope of communications interception has risen dramatically in most western countries, including Canada, in the wake of the terrorist attacks in the United States on September 11, 2001. Both the volume of intercept warrants issued and the type of information required to be intercepted have expanded. In addition, legislative changes enacted in many countries in the wake of Sept. 11 have also granted greater powers to law enforcement and national security agencies to intercept communications, including:

- In the United States, the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* (or USA *PATRIOT Act*) expands the authority of law enforcement and intelligence agencies to monitor private communications and to access personal information without a warrant.[10] The *USA Patriot Act* also redefines "foreign intelligence information" to permit more liberal sharing of information about U.S. citizens between law enforcement agencies and intelligence agencies, including the Central Intelligence Agency and the National Security Agency. Section 203(b) permits law enforcement officers to share intercepts of telephone and Internet

---

[7] *Ibid.*

[8] Gerard McManus, "We dwarf US in phone taps," *Herald Sun* (Melbourne), Sept. 15, 2002.

[9] Mark Winther and William Stofega, *The Market for Lawful Intercept Solutions: From the Circuit Switch to Next-Generation Networks and Beyond*, IDC Report #26127, December 2001.

[10] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*, Public Law No. 107-56, 115 Statutes 272, October 26, 2001. For an analysis of the wiretap provisions of the *US PATRIOT Act*, see: Charles Doyle, *The USA Patriot Act: A Legal Analysis*, U.S. Library of Congress. Congressional Research Service. Washington, D.C.: April 15, 2002. RL31377; and American Civil Liberties Union website: http://www.aclu.org/congress

conversations with the CIA without court order. And Section 203(a) permits law enforcement agencies to provide to the CIA foreign intelligence and counterintelligence information revealed to a grand jury – also without court order.

- In Canada, Bill *C-36* gives police an increased and expanded ability to monitor and conduct surveillance on communications that relate to terrorist activity. Police may now obtain surveillance warrants for suspected terrorists for one year,[11] compared to the 60-day period under provisions of the *Criminal Code*. Bill C-36 also amended the *National Defence Act* to clarify the mandate of the Communications Security Establishment (CSE) to collect foreign communications. Previously, the CSE was only allowed to monitor communications outside Canada. The Minster of National Defence is now authorized to permit interceptions of discussions between a foreigner and someone in Canada.
- Great Britain recently adopted controversial new measures that expand the release of communications records without warrant. Prime Minister Tony Blair defended the Home Office draft order to expand the list of authorities empowered to obtain the communications logs of every telephone, Internet and email user. Currently only police, the intelligence services, the inland revenue and customs and excise have that power. The new order would expand that power to include seven Whitehall departments, every local authority in the country and a host of other bodies and public organizations.[12] Each of those organizations will be able, without a court order, to compel telephone companies and Internet service providers to hand over detailed personal information on individual users under the data retention section of the United Kingdom's *Regulation of Investigatory Powers Act.*[13]

Basic customer information not private

The sanctity of confidential customer billing information has also been steadily eroded by many legal judgments well before the changes in the wake of Sept. 11. Basic customer information, such as name, billing address, phone number and name of service provider, are no longer viewed as private. The changing interpretation of confidentiality has had profound implications for law enforcement agencies, which no longer require warrants to obtain that customer information previously barred from them without a court order. Court judgments in both Canada and the United States on telephone subscriber information also

Court judgments in both Canada and the United States also establish landmark precedents that have made it legally possible for law enforcement agencies to expand the scope of warrantless interception to employ traffic data

[11] Canada. *Bill C-36*, 49-50 ER II, Nov. 28, 2001.

[12] Stuart Millar and Lucy Ward, "No 10 defends wider electronic surveillance," *The Guardian*, June 12, 2002.

[13] United Kingdom. *Regulation of Investigatory Powers Act* (RIPA), 2000, chapter 23

establish landmark precedents that have made it legally possible for law enforcement agencies to expand the scope of warrantless interception to include complex traffic data.

Initial attempts by Canadian law enforcement agencies more than a decade ago to obtain technical information on every phone company customer in advance - without legal authorization - were rebuffed by the federal regulator. The Criminal Intelligence Service of Ontario applied to the CRTC in 1990 to compel **Bell Canada** to provide customer-specific information that would facilitate the installation of DNR devices. The CRTC concluded that the information in question was "information kept by Bell Canada regarding the customer" and was therefore properly subject to the confidentiality provisions of Article 11.1 of Bell Canada's Terms of Service. The CRTC further stated:

> . . . provisions concerning the release of customer information for the purposes of law enforcement must, among other things, strike an appropriate balance between the subscriber's interest in privacy and the public's interest in law enforcement. The Commission considers that the current Article 11.1 strikes the appropriate balance between those interests. . . . The Commission considers Parliament and the courts to be the appropriate arenas for determining what are, or should be, the proper procedures for authorizing the release of the information described in CISO's applications.[14]

Courts have held that a person does not have a reasonable expectation of privacy in personal information that does not tend to reveal intimate details of his or her lifestyle

The balance shifted significantly in favour of law enforcement agencies with the Supreme Court of Canada's landmark 1993 judgment in *R. v. Plant.*[15] In that case, the court held that a person does not have a reasonable expectation of privacy in personal information that does not tend to reveal intimate details of his or her lifestyle and personal choices. That finding was similar to an earlier U.S. Supreme Court case that declared pen registers are legal because individuals do not have a reasonable expectation of privacy in their telephone numbers.[16]

That doctrine was enshrined in statute by the Parliament of Canada two years ago. The *Personal Information Protection and Electronic Documents Act*[17] allows for the disclosure of personal information without the knowledge and consent of the individual to whom it pertains, as long as that disclosure is requested by a government institution that has identified its lawful authority to obtain such information.

Citing the *Plant* case, the CRTC amended Bell Canada's Terms of Service in 2001 to permit the release of carrier identification and link information of individual phone numbers to law

---

[14] Canada. Canadian Radio-television and Telecommunications Commission. *Telecom Decision CRTC 91-2*, "Criminal Intelligence Service of Ontario – Release of Information by Bell Canada," Ottawa: 12 February 1991.

[15] Canada. Supreme Court. *R. v. Plant* (1993) 3 SCR 281.

[16] U.S. Supreme Court. *Smith v. Maryland*, 442 U.S. 735, 742 (1979).

[17] Canada. *Personal Information Protection and Electronics Documents Act (PIPEDA)*, SC 2000, Chapter 5

enforcement agencies without a warrant.[18] The commission determined that the association of a telephone number with a service provider does not disclose the identity of the subscriber – and stated that release of that information does not contravene the *Charter of Rights and Freedoms.*

Most recently, the CRTC agreed to a further change to permit warrantless access to reverse directory information.[19] Reverse directories enable the determination of customer names and addresses from a known telephone number. The CRTC sided with police arguments that reverse directories are an "important and indispensable" tool for police investigations. The CRTC also determined that the customer information in a reverse directory is not confidential. That finding enabled the CRTC to conclude in its August 2002 decision that the value of reverse directory information for law enforcement outweighs the privacy concerns raised by providing the information. Ottawa's new 'lawful access' proposals could substantially erode customer confidentiality further by extending warrantless interception to all traffic data - a requirement of a new international treaty on cyber-crime.

Ottawa embraces European Cyber-crime Convention

The desire of the federal Department of Justice to adopt new statutory measures to enable real-time interception of traffic data stems from Ottawa's signature of the Council of Europe's *Convention on Cyber-Crime* almost a year ago. Canada was invited to participate in the negotiation of the Convention as a permanent non-voting observer to the Council of Europe.[20] As of August 2002, 33 countries had signed the Convention, including Canada and most of its G8 partners. The treaty becomes binding when five states have ratified it.

The *Convention on Cyber-Crime* is an international treaty that provides signatory states with joint legal tools to help in the investigation and prosecution of computer crime, including Internet-based crime, and crime involving electronic evidence. It is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security.

---

[18] Canada. CRTC. *Telecom Order CRTC 2001-279*, "Provision of subscribers' telecommunications service provider identification information to law enforcement agencies," Ottawa: 30 March 2001.

[19] Canada. CRTC. *Telecom Decision CRTC 2002-52*, "Bell Canada – Customer Name and Address," Ottawa, 30 August 2002.

[20] The Council of Europe is an intergovernmental organization formed in 1949 by West European countries. There are now 41 member countries.

*Signatories to the EU treaty must enact domestic laws requiring service providers to cooperate in both the **collection of traffic data** and the content of communications*

The treaty also contains several provisions related to the search of computer networks and interception.[21] Article 20 (Real-time collection of traffic data) and Article 21 (Interception of content data) mandate that signatories to the EU treaty must enact domestic laws requiring service providers to cooperate in both the collection of traffic data and the content of communications. Both those Articles also mandate that the parties shall adopt such legislative and other measures to empower their law enforcement authorities to directly collect or record such content and traffic data *without the participation of the service provider*.

The *Cyber-crime Convention* ***also applies to privately-owned corporate data networks.*** In an overlooked provision of the treaty, the definition of 'service provider' in Article 1 refers to "both public and private entities that provide users of their services the ability to communicate by means of a computer system."[22]

The treaty's main objective is to pursue a common criminal policy aimed at combating cyber-crimes, especially by adopting new legislation and fostering international co-operation. The Convention aims principally at:

- Harmonizing the domestic criminal law elements of offences and connected provisions in the area of cyber-crime;
- Providing for domestic criminal procedural law powers necessary for the investigation and prosecution of offences committed by means of a computer system or evidence in relation to which is in electronic form; and
- Setting up an effective regime of international co-operation.

The EU Treaty will also be supplemented by an additional protocol making any publication of racist and xenophobic propaganda via computer networks a criminal offence.

The convention requires all signatories to adopt new laws providing for government access to encrypted information, and criminalizes the possession of common security tools. It would necessitate changing wiretapping laws in each country to facilitate the collection of information by requiring companies that provide Internet services to collect and maintain information in case it is needed by law enforcement agencies. It would also permit international access to such information by governmental

---

[21] The *Cyber-Crime Convention*, ETS No. 185, was promulgated in Budapest on Nov. 23, 2001. The full text of the proposed treaty and related documents are available at: http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm.

[22] Council of Europe. *Explanatory Report on the Convention on Cybercrime (ETS No. 185),* Strasbourg: November 8, 2001, p. 38. http://conventions.coe.int/Treaty/en/Reports/Html/185.htm

authorities in different jurisdictions. Hence, Ottawa's need to amend the *Criminal Code* before it can ratify the *Convention on Cyber-Crime*, according to the consultation paper.

Privacy advocates and civil liberties groups, including Privacy International and the Washington D.C.-based Electronic Privacy Information Center (EPIC), oppose the *Cyber-crime* treaty, arguing it grants too much power to police and does not adequately respect privacy rights.[23] EPIC believes sufficient privacy and due process protections are noticeably lacking in the treaty, posing a threat to human rights.

Yet Ottawa argues those measures are needed to prevent law enforcement agencies from falling behind in their continuing fights against terrorism, drug trafficking, organized crime, money-laundering and fraudulent telemarketing. The discussion paper points to the difference between Canada and "several" other countries, which have already updated legislation to give security authorities "lawful access capabilities." At the G-8 Justice and Interior Ministers' meeting held at Mont Tremblant, Que. in May 2002, the G-8 members[24] endorsed recommendations to trace networked communications across national borders in order to combat terrorist and criminal organizations, as well as high-tech crime. By implementing the provisions outlined in the consultation paper, Canada will be in a position to ratify the Convention contributing "to our G-8 and other global obligations."

Future Outlook

Legal requirement sought to ensure intercept capability

Several amendments to the *Canadian Criminal Code* are being proposed by the federal government to deal with the interception and search-and-seizure provisions noted above, and to permit Canada to ratify the *Cyber-Crime* treaty. There is currently no comparable legislative mechanism in Canada that can be used to compel all telecommunications carriers and Internet service providers to develop or deploy systems providing interception capability, even if a legal authorization is obtained by law enforcement or national security officials to

---

[23] American Civil Liberties Union, the Electronic Privacy Information Center and Privacy International, "Comments on Draft 27 of the Proposed CoE Convention on Cybercrime," *Submission to U.S. Department of Justice*, Washington, D.C.: June 7, 2001.

[24] Statement of the G8 Justice and Interior Ministers, "Recommendations for Tracing Networked Communications Across National Borders in Terrorist and Criminal Investigations," Mont Tremblant, Que., May 14, 2002. http://www.g8j-i.ca/english/doc2.html

The Group of 8 (G8) is made up of the heads of state of eight industrialized countries (US, UK, France, Germany, Italy, Japan, Canada & Russia plus the European Union). The leaders have met at an annual summit since 1975 to discuss issues of common importance.

intercept the communications of a specific target. The sole exception is the *Radio-communication Act*, which was amended in 1996 to require Canadian wireless providers to have facilities capable of providing intercept capability to authorities.

The central tenet of Ottawa's proposal is that all service providers will be required to have the technical capability to provide access to the entirety of any telecommunication traffic.

The central tenet of Ottawa's proposal is that all service providers (wireless, wireline and Internet) will be required to have the technical capability to provide access to the entirety of any telecommunication traffic transmitted over their facilities, subject to a lawful authority to intercept. This would include the content and the telecommunications-associated specific data associated with both circuit-based and IP-based telecommunication traffic.

Ottawa's new laws addressing the requirement for service providers to have intercept-capable transmission apparatus could, according to the Department of Justice, set out the following:

- General operational requirements describing the interception capability;
- Regulation-making authority to specify the details of the functional requirements;
- A capacity for forbearance from certain obligations; and
- A compliance mechanism.

Service providers would be solely responsible for paying the costs of buying new equipment to comply with the new laws.

Police would also be able to obtain a search warrant allowing them to find "hidden electronic and digital devices" that a suspect might be concealing. In most circumstances, a court order would be required for government agents to conduct Internet monitoring.

Data Preservation Requirement

Ottawa's proposals would also contain provisions authorizing police to order Internet service providers to retain logs of all Web browsing of a specific individual for up to six months – dubbed data preservation. The procedural mechanism of a preservation order is contained in the EU's *Convention on Cyber-Crime*, but does not yet exist in Canadian law.

Several of the provisions agreed to by G8 ministers at the Mont Tremblant meeting in May 2002 also relate to the preservation of data in order to:

- Ensure data protection legislation, as implemented, takes into account public safety and other social values, in particular by allowing retention and preservation of data important for network security requirements or law enforcement investigations or prosecutions, and

particularly with respect to the Internet and other emerging technologies.

- Permit domestic law enforcement to serve foreign preservation instructions to domestic service providers after expedited approval, with substantive review if required by domestic law, through a domestic judicial or similar order.
- Ensure the expeditious preservation of existing traffic data regarding a specific communication, whether one or more service providers were involved in its transmission, and the expeditious disclosure of a sufficient amount of traffic data to enable identification of the service providers and path through which the communication was transmitted, through the execution of a single domestic judicial or similar order where permitted by domestic law.
- Authorize domestic law enforcement to use the mechanisms described in the prior paragraph to respond to a foreign request, through expedited mutual assistance, even if there is no violation of the domestic law of the requested State.[25]

The idea behind data preservation is to preserve select communications traffic information on targeted individuals or groups for law enforcement agencies to ensure that information pertaining to an investigation isn't accidentally deleted before they have a chance to get a search warrant to actually view the file logs. A preservation order acts as an expedited judicial order and is temporary, remaining in effect only as long as it takes law enforcement agencies to obtain a judicial warrant to seize the data or a production order to deliver the data.

Ottawa's proposals would legally obligate ISPs to have the technical capability to keep and to produce a record of an individual's Internet traffic data – such as Web surfing and e-mail history - upon request. Canada's *Criminal Code* would also have to be amended to give police appropriate procedural powers to gain that traffic information – either through a general or specific production order.

Data retention on EU's table

Law enforcement agencies in many countries - including agencies of the EU - have also urged the adoption of more sweeping "data retention" requirements, which would compel all telecommunications and Internet service providers routinely to

[25] The phrase "even if there is no violation of the domestic law of the requested State" is intended to signify that the requested State should provide assistance even if the conduct at issue does not meet all the conditions to qualify as a crime or cannot otherwise by prosecuted as a crime in that State.

capture and archive information detailing the telephone calls, e-mail messages and other communications of their users.

Data retention would compel service providers to collect and retain a range of data concerning ***all subscribers.***

Unlike preservation orders that are specific to certain individuals, traffic data retention is a general requirement that would compel service providers to collect and retain a range of data concerning *all subscribers*. While many providers currently retain limited traffic data information for billing and other business-related purposes for short periods, there are currently no government-imposed retention requirements in the major industrialized countries.

However, the EU has recently considered adopting requirements that would force providers to *retain* certain real-time traffic data for a minimum period so that data may be used for law enforcement or national security purposes. The EU Forum on Cyber-crime released a discussion paper on the issue last November.[26] More recently, in what is viewed as a sweeping reversal of their original opposition to data retention, members of the European Parliament voted in late May to allow each EU government to enact laws to retain traffic and location data.[27] The plan, drafted in Brussels, was leaked to *Statewatch*, an independent group monitoring threats to privacy and civil liberties in the EU. The directive is regarded as a victory for both London and Washington, who have each favoured a compulsory EU-wide data retention regime.[28]

The EU's 2002 Telecommunications Privacy directive reverses a 1997 directive by allowing individual EU countries to compel telecommunications and Internet service providers to record, index, and store their subscribers' communications data.[29] The data to be retained, termed 'traffic data,' is defined to include all data generated by the conveyance of communications on an electronic communications network as well as data indicating the geographic position of a mobile user ('location data').[30] Those traffic data retention measures do not apply to the contents of communications. However, traffic data includes information identifying the source, destination, and time of a communication, as well as the personal details of the subscriber of any communication device.

---

[26] European Commission. *EU Forum on Cybercrime*. "Discussion Paper for expert's Meeting on Retention of Traffic Data," Brussels: 29 October 2001.

[27] The European Parliament. Council of the European Union. *Directive 2002/58/EC*, "Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector," Brussels: 12 July 2002. http://www.gilc.org/as_voted_2nd_read.html

[28] See: Sarah Anrews (ed.), *Privacy and Human Rights 2002: An International Survey of Privacy Laws and Developments*, Electronic Privacy Information Center and Privacy International. Washington, D.C. and London: 2002, pp. 43-4.

[29] Council of the European Union. *Directive 2002/58/EC, supra.*, Article 15(1).

[30] *Ibid*, Articles 2(b) and 2(c).

A proposal currently before the EU would require all service providers to retain communications data for law enforcement purposes for up to two years

The proposal currently before the EU would require all service providers to retain communications data for investigative purposes for at least one year and a maximum of two years. The directive would also allow governments to compel service providers to retain that information without any specific judicial authorization. EU countries would have until October 31, 2003 to implement the Directive and several members (Belgium, France, Great Britain and Spain) have already provided for the retention of electronic communications data.

Yet Denmark, the current holder of the rotating EU presidency, recently denied that in-depth guidelines were under consideration and said it was only consulting member states on how to bring their rules on data retention into line with each other. "The proposal contains no detailed information as to what the contents of such rules should be," the Danish Presidency of the EU, said in a statement.[31] He was referring to a consultation document sent out to member states in June, which urges approval of measures allowing EU countries to harmonize their rules on the obligations of telecommunications companies to retain traffic data.

Complex data traffic types

That denial, however, flies in the face of a confidential agenda for a meeting of law enforcement experts on a proposal for "a common European Union law" on data retention. That meeting, held at the EUROPOL headquarters in The Hague on April 11, 2002, considered a wish list for the type of communications traffic data that European law enforcement authorities would like to obtain from ISPs and telephone companies[32] EUROPOL (European Police Office) is the EU's law enforcement organization that handles criminal intelligence.

The EU directive would apply data retention rules to any communications device and service, including landline phones, mobile phones, smart handheld devices, faxes, e-mails, chatrooms – even wireless SMS Internet-based

The retention of such vast amounts of data, however, is hugely complex and problematic for service providers. The EU directive would apply data retention rules to any communications device and service, including landline phones, mobile phones, smart handheld devices, faxes, e-mails, chatrooms – even wireless SMS Internet-based text messages. The nine-page EUROPOL list details a bewildering array of traffic data types generated by users and service providers that police and security agencies want service providers to retain (see Appendix 1 at the end of this study). One source has identified more than 700 types of Internet service elements alone that would be impacted. Then there are special technical issues, such as the need for time synchronization of all telecom and ISP servers, raised by the need for traffic data retention.[33]

[31] The Danish EU Presidency, *News Release*, Aug. 22, 2002.

[32] EUROPOL. "List of minimum and optional data to be retained by service providers and Telcos," *Questionnaire for Expert Meeting on Cyber Crime: Data Retention*, The Hague, 28 December 2001, File 5121-20020411LR.

[33] EUROPOL, op. cit., pp. 8-9.

For each fixed phone line, telephone companies would have to keep the following information: numbers called (whether connected or not); date, time and length of call; name, date of birth, address and bank account of the subscriber; and types of connection the user has. Wireless and satellite operators would have to keep the same information plus the "identification and geographical location" of the user - the latter detail means usage logs for each call must include geographical positioning information.

The privacy implications of such schemes are profound. "The traffic data of the whole population of the EU - and the countries joining - is to be held on record. It is a move from targeted to potentially universal surveillance," warned Tony Bunyan, *Statewatch* editor.[34]

Ottawa has not yet specified what technical standards it may adopt

Exactly how Ottawa expects service providers to implement the requirements of the *Cyber-crime Convention*, however, remains an open question. Although the Department of Justice consultation document states that details could be specified in regulations to be issued by the federal cabinet after the requisite legal changes are made, Ottawa has not yet specified what technical intercept standards it may adopt.

U.S. CALEA & J-Standard

An international cooperation program run by the U.S. Federal Bureau of Investigation, however, has already led to the promulgation and widespread international adoption of a technical standard for network-based surveillance - the FBI's so-called *CALEA* "J-standard." The United States government has led a worldwide effort over the past 15 years to enhance the capability of western police and intelligence services to intercept packet-based as well as voice communication traffic. Central to that effort is the promotion of new laws and technical standards that make it mandatory for all communication equipment manufacturers and network service providers to build surveillance capabilities in to their products and network elements.

The United States enacted those requirements in the *Communications Assistance for Law Enforcement Act* (*CALEA*).[35] Service providers are required by *CALEA* to upgrade all network equipment installed prior to Jan. 1, 1995 to enable a standardized intercept protocol – the J-STD-025

---

[34] Cited in: Richard Norton-Taylor and Stuart Millar, "Privacy fear over plan to store email," *The Guardian*, August 20, 2002.

[35] *CALEA*, enacted in 1994, was the first U.S. statute to impose upon telecommunications carriers an affirmative obligation to modify and design their equipment, facilities, and services "to ensure that new technologies and services do not hinder law enforcement's access to the communications of a subscriber who is the subject of a court order authorizing electronic surveillance."

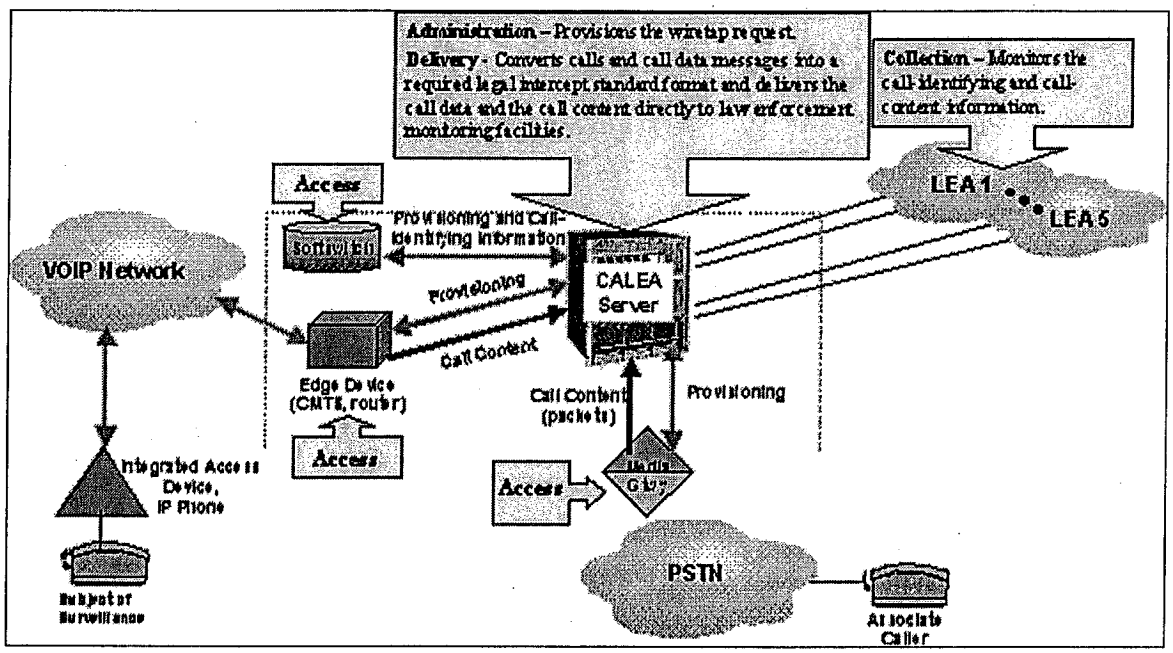
standard (see Appendix 2 at the end of this study for a detailed description). Among the general requirements of intercept systems specified by the J-standard are the following:

- Access to the entire transmitted message.
- Access to traffic-associated data generated to process any call or message.
- Full-time monitoring capability for the interception of telecommunications.
- Network operators/service providers interfaces from which the intercepted communications can be transmitted to the law enforcement monitoring facility.

(Figure 1 below illustrates the operation of a server-based J-standard system on an IP-based network.)[36]

Figure 1

***CALEA* J-Standard Server-Based System for Interception of Messages on Packet Voice Network**



Source: IDC, 2002

Although *CALEA* applies only to pre-Internet telecommunications companies, the J-standard describes collection capabilities regardless of whether telecommunications are carried on circuit or packet-based networks. The *USA Patriot Act* also provides U.S. law

[36] U.S. Department of Justice. Federal Bureau of Investigation. CALEA Implementation Section. *CALEA Flexible Deployment Assistance Guide* (3rd edition). Chantilly, Va.: May 2002, p. 4. http://www.askcalea.net/

enforcement agencies with additional authority to intercept messages sent over the Internet.

The European Union approved a secret resolution adopting the so-called ILETS standard – based on the J-standard - in early 1995 that led to a joint EU – U.S. Memorandum of Understanding signed by Canada and Australia.[37] That resolution specifies the International User Requirement (IUR) for the Lawful Interception of Communications.[38] The EU's IUR standard encompasses a much broader network-tagging system that not only provides the name, address, and phone number of subjects and associates but also e-mail addresses, credit card details, PINs, passwords, and integration of mobile phone data to create a comprehensive geographic location tracking system.[39]

Fusion with Carnivore & Echelon

Adoption of the EU *Cyber-crime Convention* has also heightened concerns associated with two broader U.S.-based interception schemes. The first, aimed at law enforcement, is *Carnivore* - an FBI-developed device to filter e-mail messages in bulk to look for specific targeted messages. The second is a foreign intelligence initiative, dubbed *Echelon,* run jointly by agencies in the United States, Great Britain, Canada and Australia to monitor global communications.[40]

Carnivore is akin to an online pen register that collects URLs.

First disclosed during a Congressional hearing in April 2000, *Carnivore* is a "packet sniffer" originally intended to assist the FBI with its surveillance operations and aimed primarily at antiterrorist activities. *Carnivore* is akin to an online pen register that collects URLs. Industry trade organizations and some carriers have suggested that *Carnivore* (now called DCS 1000)

---

[37] ILETS is the International Law Enforcement Telecommunications Seminar held annually at the FBI research facility in Quantico, Va., and includes representatives from Canada, Australia and the European Union. See: James Dempsey, "Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy," *Albany Law Journal of Science & Technology*, 8:1 (1997); and: Electronic Privacy Information Center and Privacy International. *Privacy and Human Rights 2002: An International Survey of Privacy Laws and Developments*, Washington, D.C. and London: 2002, pp. 35-6. http://www.privacyinternational.org/

[38] Council of the European Union, *Resolution on the Lawful Interception of Telecommunications*, 17 January 1995 (96/C329/01).

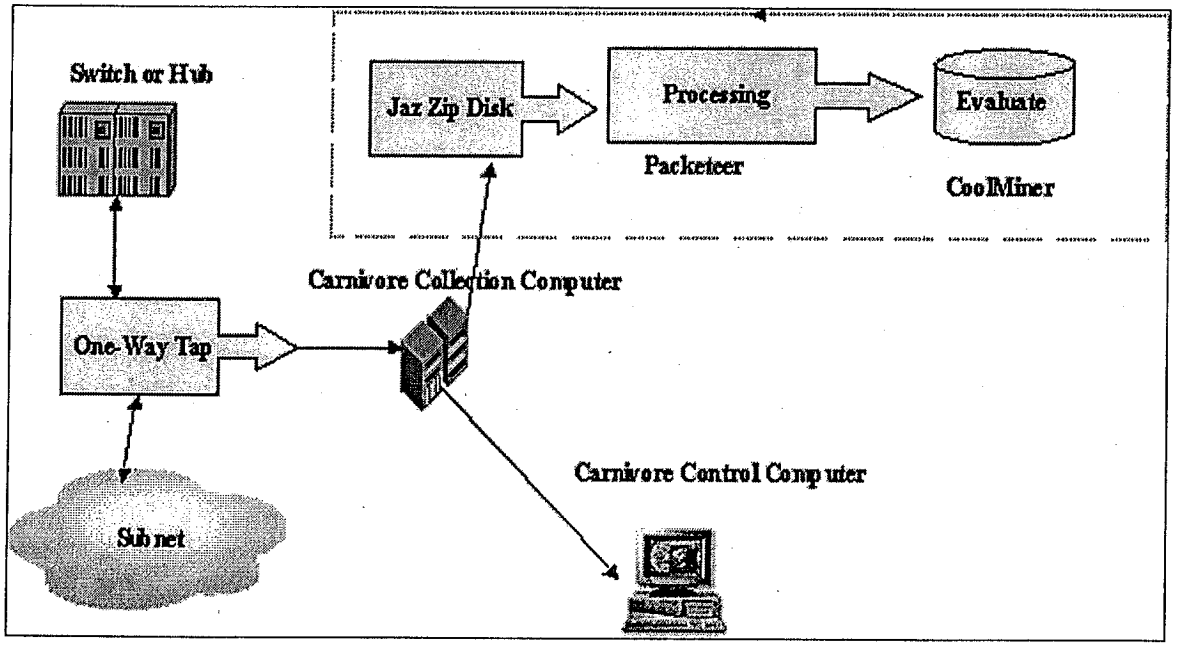
[39] European Telecommunications Standards Institute (ETSI) standard ES 201-671.

[40] Established under the 1947 UKUSA Agreement on Signals Intelligence Collection, Canada's role in *Echelon* is managed by the Communications Security Establishment (CSE) - the SIGINT agency of the Department of National Defence. The overall *Echelon* program is led by the U.S. National Security Agency (NSA) and other partners are Great Britain's Government Communications Headquarters (GCHQ) and Australia's Defence Signals Directorate (DSD).

could be deployed by telecommunication service providers as an intercept solution on next-generation IP-based networks.

Carnivore monitors data flow and saves the relevant packets according to filtering parameters. Packets may be filtered by IP address (either fixed or dynamic), protocol, text strings, TCP/UDP port, and e-mail addresses. *Carnivore* also has two post-processing applications, Packeteer and CoolMiner – collectively termed the "DragonWare" suite. Packeteer processes the raw output, reconstituting higher-level protocols from IP packets. CoolMiner develops statistical summaries and displays either pen register or full content information that is accessible via an Internet browser. *Carnivore* uses a PC running Windows NT at an ISP's office and can monitor all traffic about a user including e-mail and browser use (see Figure 2 below).[41] *Carnivore* remains under the exclusive control of government agents, who also have the ability to access the system – and an ISP's network – remotely.

Figure 2
U.S. FBI *Carnivore* Interception Architecture

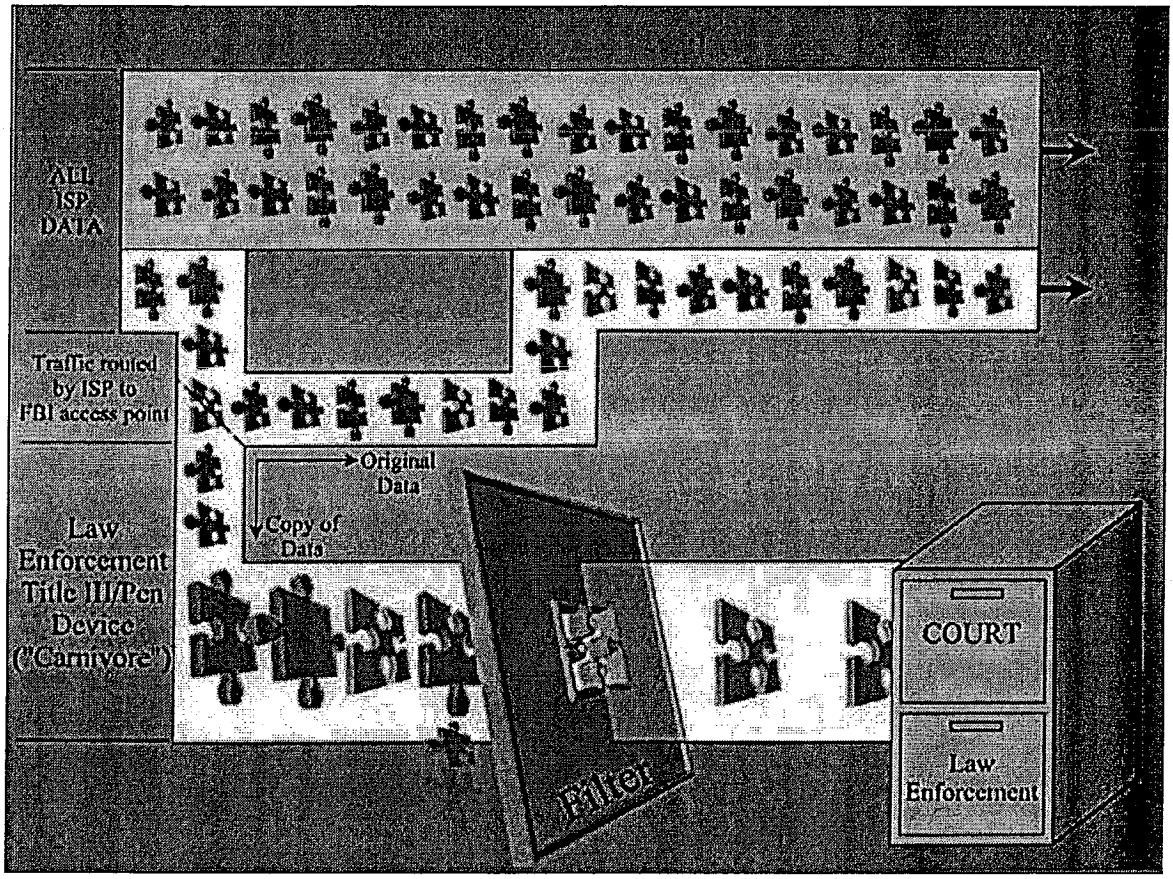


Source: U.S. Federal Bureau of Investigation; IDC, 2002

[41] Donald M. Kerr, "Internet and Data Interception Capabilities Developed by the FBI," *Statement for the record*, U.S. House of Representatives, Committee on the Judiciary, Subcommittee on the Constitution, Washington, DC: 24 July 2000, at: http://www.fbi.gov/congress/congress00/kerr072400.htm. The FBI maintains a Web page on Carnivore at: http://www.fbi.gov/hq/lab/carnivore/carnivore.htm

The FBI claims that *Carnivore* provides a "surgical" ability to intercept and collect only the communications that are the subject of a lawful order while ignoring those communications they are not authorized to intercept (illustrated in Figure 3).

Figure 3
U.S. FBI *Carnivore* 'Packet Sniffer' Filter



Source: U.S. Federal Bureau of Investigation, 2002

"*Carnivore* serves to limit the messages viewable by human eyes to those which are strictly included within the court order," states the FBI's description of the system.

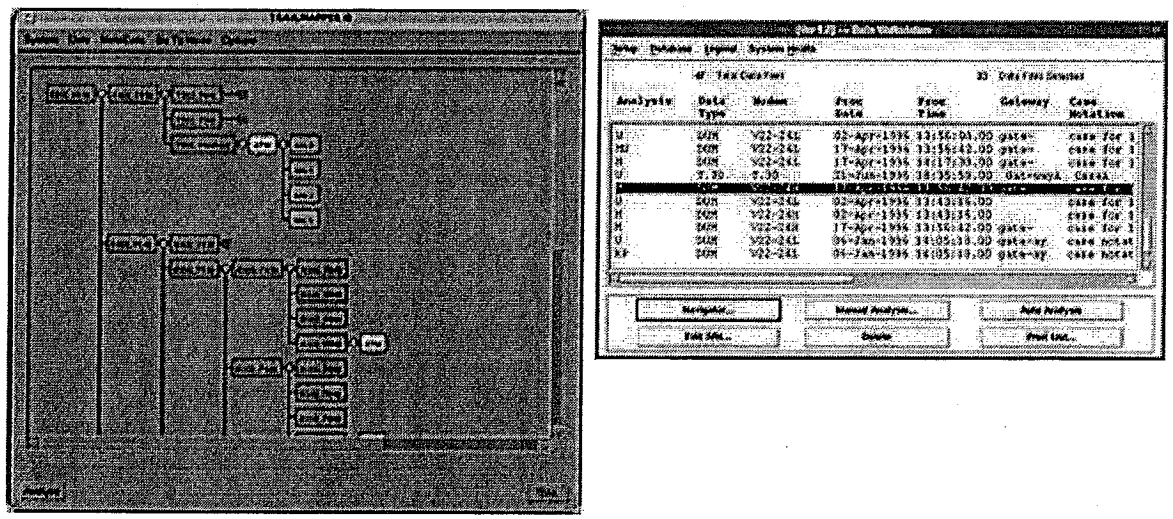
Yet that description ignores a chief criticism leveled against *Carnivore* by both privacy advocates and service providers: Allowing direct access to a service provider's network to conduct surveillance provides police with the ability to conduct broad sweeps of network communications with only their unsupervised assurance that they will only collect data which they are lawfully entitled to collect. *Carnivore* marks "a radical departure from the principle that service providers must keep government agencies out of their systems," James Dempsey, senior staff counsel to the Center for Democracy and

Technology, stated in testimony to a U.S. Senate Committee. "It invites abuse of the most invasive investigative powers."[42] Since the passage of the *USA Patriot Act,* domestic law enforcement agencies such as the FBI are now permitted to share any information they derive from interception tools such as *Carnivore* with intelligence agencies. Allied electronic intelligence agencies, including Canada's CSE, maintain a powerful interception system code-named *Echelon* that is much more sophisticated and ubiquitous than *Carnivore.*[43] *Echelon's* 'Trailmapper' software, developed by the NSA, is designed to detect activity on any targeted network – public or private. *Echelon's* associated workstation message extraction software filters, flags and preserves any message containing a targeted phrase or destined to, or originating from, a targeted location (illustrated in Figure 4).

CDA

Figure 4

***Echelon* 'Trailmapper' Network Detection and 'Data Workstation' Message Extraction Software**



Source: Applied Signal Technology Inc., 2002

[42] James Dempsey, "The Carnivore Controversy: Electronic Surveillance and Privacy in the Digital Age," *Testimony to the U.S. Senate Judiciary Committee*, September 6, 2000. Washington, D.C.: Center for Democracy and Technology, http://www.cdt.org/

[43] The European Parliament. Council of the European Union. Temporary Committee on the ECHELON Interception System. *Draft Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System)*, 18 May 2001, PE 305.391. For a comprehensive description of the SIGINT institutions and technical collection systems at the heart of *Echelon* and employed by members of the UKUSA alliance, see: Jeffrey T. Richelson and Desmond Ball, *The Ties That Bind: Intelligence Cooperation Between the UKUSA Countries*, Boston: Unwin Hyman, 1985.

Many observers fear the consequences of the merger of the global *Echelon* signals intelligence system with J-standard-based domestic law enforcement systems. Yet, that fusion has already accelerated in the wake of Sept. 11 with the increased blurring of the activities of law enforcement and national security agencies.

The merger of national security and law enforcement interception capabilities may compromise national control over surveillance activities – as well as raise the prospect of the UKUSA signals intelligence apparatus being targeted against individuals exercising legitimate rights of dissent. "The creation of a seamless international intelligence and law enforcement surveillance system has resulted in the potential for a huge international network that may, in practice, negate current rules and regulations prohibiting domestic communications surveillance by national intelligence agencies," states the latest annual international survey of privacy and human rights issues published by two leading privacy advocacy groups.[44]

For service providers, that potential fusion raises yet another problematic issue related to the controversial issue of traffic data retention. A previously classified directive governing the collection of signals intelligence by the U.S. NSA specifies a much longer retention period - of five years or more (see Appendix 3).[45]

Service providers must bear costs of intercept capability

The issue of costs associated with the new intercept measures required by both the EU *Cyber-Convention* and Ottawa's 'Lawful Access' proposal is hugely troublesome – for service providers and, ultimately, their customers. Numerous smaller ISPs fear the very real prospect that the added expense to upgrade their systems could drive them out of business.

*Under the **Cyber-Crime convention**, countries are not required to pay the costs imposed on third parties for electronic surveillance*

Privacy advocates and legal experts share the concerns of industry players over the EU's and Ottawa's proposals. "Requiring that law enforcement pay for their surveillance provides an important level of accountability through the budget process each year," states a joint brief by EPIC, Privacy International and the American Civil Liberties Union submitted to both the Council of Europe and the U.S. Department of Justice. Under Article 15.3 of the EU Council's *Cyber-Crime convention*, however, countries are not required to pay the costs

[44] Sarah Andrews (ed.), *Privacy and Human Rights 2002: An International Survey of Privacy Laws and Developments*, Electronic Privacy Information Center and Privacy International, Washington, D.C. and London: 2002, pp. 52-3. http://www.privacyinternational.org/

[45] U.S. National Security Agency. *United States Signals Intelligence Directive 18*, Fort George Meade: 27 July 1993. (Declassified from Secret). Available from the Federation of American Scientists at http://www.fas.org/

imposed on third parties for their demands for electronic surveillance. "This both significantly lowers barriers to law enforcement surveillance by removing any limits on how much surveillance can be afforded and is grossly unfair to the providers," states the ACLU-EPIC brief.[46]

Yet, the federal government's consultation document appears to reject the call of industry players for inclusion of a reimbursement requirement. Under Ottawa's proposals, all communication providers would be required to provide "a basic intercept capability" when providing any new service to the public. Service providers would be responsible for the costs associated with ensuring that any new equipment provides agencies such as the RCMP and CSIS with unfettered access to electronic messages or phone conversations. However, the discussion paper hints that carriers may not have to bear the financial burden of upgrading existing systems.

Although *CALEA*/ETSI-compliant software generics are bundled into all new switching gear, most equipment vendors are tight-lipped about the price of their intercept systems. IDC research, however, suggests *CALEA*/ETSI-compliant software ranges from between US$50,000 to US$500,000 - depending on the traffic volume handled by an upgraded switch. The price of server-based adjunct solutions for TDM and IP networks typically begins at US$200,000 and scales upward to millions of dollars, depending upon the size of the carrier and the number of switches supported.[47]

Service providers must have a better understanding of the costs that the proposals will carry. "The paper is very vague on many issues, including costs," said Sheridan Scott, chief regulatory officer at **Bell Canada**. "We don't know what the price tag looks like exactly or what the impact would be on subscribers. But there could be a huge problem for us associated with the cost of any potential scheme that would require service providers to keep data for any amount of time."[48]

Bell Canada would also oppose any traffic data retention proposal, says Bernard Courtois, executive vice-president and chief legal counsel. "Apart from the complexity and costs of such a scheme, we question whether it would serve any useful purpose to government or police agencies."[49] Ms Scott also challenged Ottawa to clarify its objectives on retention of traffic data. "The consultation document is very vague on this critical issue and does not specify what its goals are *vis-à-vis* the EU."

---

[46] American Civil Liberties Union, the Electronic Privacy Information Center and Privacy International, "Comments on Draft 27 of the Proposed CoE Convention on Cybercrime," *Submission to U.S. Department of Justice and CDPC of the Council of Europe*, Washington, D.C.: June 7, 2001, p. 2.

[47] Winther and Stofega, IDC Report #26127, *op.cit.*

[48] Sheridan Scott, Interview, Toronto, October 17, 2002.

[49] Bernard Courtois, Interview, Toronto, Sept. 19, 2002 and October 17, 2002.

Similar concerns were raised two years ago by major telecom providers in the United Kingdom. Both **BT PLC** and **Vodafone** stated that changes to Great Britain's communications interception law did not set out in detail what is expected of carriers when served with a warrant. BT also queried why the new measures did not discuss cost issues.[50]

The proposals for blanket traffic data interception and retention are hugely problematic, says an official at **Rogers AT&T Wireless** who asked not to be identified.[51] The cost issue alone is considerable. Rogers AT&T Wireless calculates that simply providing a raw "siphon tap" capability across its entire network would cost over C$12-million.

There are additional network issues that impose further complexity and costs on wireless carriers, such as encryption, for example. GPRS wireless networks have four levels of encryption, "so a key question for an operator is, at what level do you provide LEA access?" the Rogers AT&T official said.

Service providers fear storage requirements of 'plug, play and peek'

Telecommunications and Internet service providers are unanimous in decrying the onerous storage requirements that would be imposed on them by Ottawa's adoption of the EU Convention and possibly magnified by EUROPOL's traffic data retention proposals. "It's ludicrous to think service providers should have to keep such a vast amount of data," said the Rogers AT&T official. "And the logistical problems associated with data retention are compounded by the longer time periods advocated by the EU."

Consider one statistic provided by a Canadian ISP. Every ISP currently logs its customers' IP address and records the 'start' and 'stop' time of their Internet use in order to bill for the service. That simple metric alone generates 450 Megabytes of data per month for one small-size ISP with 10,000 customers, said Bob Carrick, president of directory **Canadian ISP.com.**[52] Yet the average Internet customer produces between three to five gigabytes of traffic and message data per month. A small ISP with only 10,000 customers would need 300 terabytes of storage capacity simply to meet a traffic data retention requirement of six months. The EU proposals seeking retention for two years boost that storage need to the pica-byte range.

A small ISP with only 10,000 customers would need 300 terabytes of storage capacity simply to meet a data retention period of six months.

That means even the smallest ISP would require multiple servers to retain and store that data, as well as need additional

[50] See: United Kingdom. Secretary of State for the Home Department. *Interception of Communications in the United Kingdom: A Consultation Paper.* London: June 1999.

[51] Interview, not for attribution, Toronto, Sept. 24, 2002.

[52] Bob Carrick, cited in: Shane Schick, "Surveillance may force ISP upgrades," *Communications & Networking*, October 2002, p., 6.

server capacity to maintain network speeds. The scale of this issue is huge, considering that almost one-half, or 450, of Canada's 950 ISPs serve more than 1,000 customers.

"We obviously would have concerns about how much it's going to cost, and who's going to bear those costs," said Jay Thomson, president of the Canadian Association of Internet Providers. Some Canadian ISPs would have to modify their systems significantly to meet those new requirements. "But it's a big black hole," Mr. Thomson said. "We don't know who will have to do what, or how much it will cost. We also have concerns about what the potential obligations could mean for our customers and their right to privacy."[53] The greatest fear of ISPs is that intercept measures will stall Internet growth – and impede the use of e-commerce.

The greatest fear of ISPs is that intercept measures will stall Internet growth – and impede the use of e-commerce.

Rogers AT&T echoes the storage concerns of the ISPs. "Figuring out how to keep and store all that information on every customer would not be easy or cheap," said the Rogers AT&T official. "And, ultimately, it may not prove to be of any use to law enforcement agencies unless they are able to sift through and act upon all the information that would be generated."[54]

The language in Ottawa's consultation document is so vague that it could be used to justify unprecedented intrusion into personal privacy, Mr. Carrick warns. "The one line that worries me, 'A preservation order . . . requires service providers ... to store and save existing data.' Does that mean data that they've already been tracking? It's the words 'existing data' that really and truly bother me."[55]

The Electronic Privacy Information Center (EPIC) also objects to Ottawa's proposals. Sarah Andrews, an analyst specializing in international law at EPIC, says Ottawa's discussion paper goes beyond what the European *Cyber-crime* treaty specifies. "Their proposal for intercept capability talks about all service providers, not just Internet providers," Ms Andrews told *CNET.com*.[56]

Michael Geist, a professor at the University of Ottawa who specializes in e-commerce law, says that the justification for adopting such sweeping changes to Canadian law appears weak. "It seems to me that the main justification they've given for all the changes is that we want to ratify the *Cyber-crime* treaty and we need to make changes. To me, that's not a particularly convincing argument. If there are new powers needed for law enforcement authority, make that case." He added, "there's nothing in the document that indicates (new

---

[53] Cited in: Oliver Moore, "Ottawa Poised to become Big Brother," *Globe and Mail Update*, September 3, 2002, http://rtnews.globetechnology.com/

[54] Interview, *op. cit.*

[55] Cited in: Moore, *op. cit.*

[56] Cited in: Declan McCullagh, "Will Canada's ISPs become spies?" *CNET News.com*, August 27, 2002.

powers) are needed. I don't know that there have been a significant number of cases where police have run into problems."[57]

Civil libertarians also share that criticism. "There's really no need for additional powers to be granted," said Darrell Evans, executive director of the B.C. Freedom of Information and Privacy Association in Vancouver. "Do Canadians really want to create a surveillance society?"[58]

The call for a national database in the report – a proposal requested by the Canadian Association of Chiefs of Police - is much more contentious. In May 2000, the Human Resources Department dismantled a massive database on citizens that could have contained up to 2,000 pieces of information on every citizen after news of its existence triggered a wave of indignation and protest from Canadians. Gus Hosein, an activist with Privacy International and visiting fellow at the London School of Economics, termed the proposed database "a dumb idea."[59]

Ironically, western Internet monitoring schemes resemble China's ambitious Golden Shield *content-filtering and surveillance scheme.*

Ironically, those western Internet monitoring schemes resemble the ambitious *Golden Shield* content-filtering and surveillance scheme currently being implemented in the People's Republic of China.[60] Perhaps the harshest criticism of the EU's framework for data retention comes from the European Data Protection Commissioners, who fear the prospect of telecommunications and Internet service providers becoming an arm of the police.

The commissioners recently expressed what they termed "grave doubt as to the legitimacy and legality" of any broad measure that would require mandatory, systematic retention of traffic data. Even in an isolated specific case, the commissioners state there must be a demonstrable need for traffic data retention, the period of retention must be as short as possible and the practice must be clearly regulated. "Systematic retention of all kinds of traffic data for a period of one year or more would be clearly disproportionate," they stated in a news release, adding such a measure "would be an improper invasion of human rights."[61]

There is a growing chorus that initiatives such as the EU's proposals and the federal government's 'Lawful Access' plan, coupled with post-Sept. 11 laws, have shifted the balance too

---

[57] Cited in: McCullagh, *Ibid.*

[58] Darrell Evans, cited in: Kevin Restivo, "Ottawa Mulls Tracking Internet Usage," *National Post*, August 30, 2002.

[59] Gus Hosein, cited in: McCullagh, *op. cit.*

[60] The *Golden Shield* Project was launched by the Ministry of Public Security in Nov. 2000 at the Security China trade show in Beijing. See: Andrews, *op. cit.*, pp. 156-8.

[61] European Data Protection Commissioners. "Statement on Mandatory Systematic Retention of Telecommunication Traffic Data," Cardiff: 11 September 2002.

far away from respect of individual privacy in favour of protecting society. The desire of governments to exploit network technology in the interest of fighting terrorism may also ultimately prove Quixotic without a more enlightened approach. As Canada's Privacy Commissioner, George Radwanski, recently stated:

> We must guard against the eagerness of law enforcement bodies and other agencies of the state to use the response to September 11 as a Trojan horse for acquiring new invasive powers or abolishing established safeguards simply because it suits them to do so. . . .
>
> Who would sift through all that additional information? Imagine the resources it would take. . . . We'd only be creating a thicker forest of information in which the terrorists could hide. . . . What is needed, to make us safer from terrorism, is not mindless invasion of privacy, but more and better intelligence.[62]

[62] George Radwanski, Privacy Commissioner of Canada, "Remarks to Internet Law & Policy Forum Conference," Seattle: September 19, 2002.

Essential Guidance: Issues & Questions for Service Providers to Consider

The federal Department of Justice is accepting comments on its consultation paper until November 15. Legislative proposals based on the paper could be introduced to Parliament by early next year. Yet industry players need much more detailed consultation with government, as well as an opportunity to examine actual proposed legislative amendments, in order to better understand what may be required of them.

Among the issues related to Ottawa's lawful intercept proposals that each service provider should consider are:

General regulations and technical standards

- What technical standards for traffic interception will Canadian service providers use? Does the federal government plan to specify those requirements by statute or subsequent regulation?
- Will definitions be functional, irrespective of any particular technology?
- What impact would Ottawa's proposed requirements have on a service provider's business? Would Canadian firms be placed at a competitive disadvantage?
- Will the new intercept requirements be transparent to the entire business community and enforced uniformly?
- Should service providers be expected to do all the processing required? Do law enforcement and security and intelligence agencies have enough expertise and trained personnel to process the intercepted material?
- Is it reasonable to impose the cost of providing intercept capability and data preservation in any new network equipment on service providers?
- What is the magnitude of those costs and what is the potential impact on individual service customers?
- Could telecommunications service providers be permitted to recover lawful intercept costs and associated network modification expenses from the existing monthly surcharge levied on all telephone customers to provide access to 911 emergency service?
- Should there be a role for equipment vendors in educating service providers about lawful access operability?

Preservation orders

- Should a data-preservation order apply only to stored computer data or should it also apply to paper records?

- Under what legal standard should a data-preservation order be granted?
- Should standards vary depending on the nature of the data?
- Who should be authorized to issue a preservation order?
- Should there be a specific penalty for non-compliance with a preservation order, or is contempt of court sufficient?
- Should there be a maximum period that an ISP can be required to preserve Web surfing history? What is a reasonable period for data preservation?
- For how long should a law enforcement official be able to impose a preservation order on service providers?

General production orders

- Should the *Criminal Code* be amended to allow law enforcement officials to obtain production orders in specific cases?
- Should the *Criminal Code* allow for anticipatory orders (e.g., permit law enforcement agencies to monitor transactions for a specified period of time)?
- What procedural safeguards are required?

Specific production orders

- Should there be a specific power, parallel to the provision in the *Criminal Code* related to dial number recorders, to allow law enforcement and national security agencies to obtain IP-based traffic data?
- How should "traffic data" be defined? Should the definition of traffic data be combined with telephone-related information and addressed in the same *Criminal Code* provision?
- Should other specific production orders be created under a lower standard?
- What kind of procedural safeguards are needed?

Further EU agreements on traffic data retention

- What is the federal government's intention and policy on traffic retention? Will Ottawa be compelled to adopt any subsequent EU traffic data retention scheme because of ratification of the EU *Cyber-Crime Convention*?
- Which traffic retention proposals does the Council of the European Union intend to adopt and for what length of time would service providers be obligated to *retain* real-time traffic data?

- Should the federal government be permitted to impose comprehensive traffic data retention requirements on service providers affecting all of their subscribers – and without warrant?
- What traffic data elements do law enforcement and national security agencies legitimately need to exercise their duties?
- Does real-time tracking of Internet URLs and Web-browsing activities reveal the content of a customer's communications?
- Does current case law give Canadians a reasonable expectation of privacy that their Web-surfing activity should remain privileged? What obligations are imposed on service providers to protect that information?
- What are the costs to a service provider associated with a data retention scheme? What is the potential impact on individual customers?

National database

- Should the federal government be permitted to create a centralized database on every Canadian Internet user?
- If such a database were created, who should maintain it?
- If confidential customer information shared among affiliated companies is stored in and accessed from a centralized database, does that raise any particular privacy issues for a service provider?
- Should there be any restrictions on the collection and storage of subscriber information in such a database?
- What conditions should govern access to such a database?

Compliance and Intercept-free havens

- Should companies who provide anonymous Internet access be compelled to gather customer information and traffic data? Should intercept-free havens be permitted?
- What kind of compliance mechanism should be established?
- Who should oversee compliance?
- What penalties will be imposed on service providers that do not comply with any new lawful intercept measures?

Learn More

References & Further Reading

American Civil Liberties Union, the Electronic Privacy Information Center and Privacy International, "Comments on Draft 27 of the Proposed CoE Convention on Cybercrime," *Submission to U.S. Department of Justice and CDPC of the Council of Europe*, Washington, D.C.: June 7, 2001.

Sarah Andrews (ed.), *Privacy and Human Rights 2002: An International Survey of Privacy Laws and Developments*, Electronic Privacy Information Center and Privacy International. Washington, D.C. and London: 2002, http://www.privacyinternational.org/

Kristin Archik, *Cybercrime: The Council of Europe Convention*, U.S. Library of Congress. Congressional Research Service. Washington, D.C.: April 26, 2002. RS21208.

Lisa Austin, "Is Privacy a Casualty of the War on Terrorism?" in: Ronald Daniels et. al. (eds.), *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill,* Toronto: University of Toronto Press, 2001, pp. 251-67.

Australia. Attorney-General. *Telecommunications Interception Act Report for the year ending 30 June 2001,* Canberra: September 2002.

Belgium. "Draft Framework Decision on the retention of traffic data and on access to this data in connection with criminal investigations and prosecutions," Proposal to Council of the European Union. European Parliament. June 2002: Confidential. Available at: http://www.statewatch.org/

Duncan Campbell, "Interception Capabilities 2000: The State of the Art in Communications Intelligence of Automated Processing for Intelligence Purposes of Intercepted Broadband Multi-Language Leased or Common Carrier Systems, and its Applicability to COMINT Targeting and Selection, Including Speech Recognition," Working document for the STOA Panel. European Parliament. Director General for Research, Scientific and Technical Options Assessment Programme Office, *Development of Surveillance Technology and Risk of Abuse of Economic Information*, vol. 2. Luxembourg: Dec. 1999. PE 168.184/v2

Canada. Canadian Radio-television and Telecommunications Commission. Canada. *Telecom Decision CRTC 2002-52*, "Bell Canada – Customer Name and Address," Ottawa, 30 August 2002.

----------. *Telecom Order CRTC 2001-279*, "Provision of Subscribers' Telecommunications Service Provider Identification Information to Law Enforcement Agencies," Ottawa: 30 March 2001.

----------. *Telecom Decision CRTC 91-2*, "Criminal Intelligence Service of Ontario – Release of Information by Bell Canada," Ottawa: 12 February 1991.

Canada. Department of Justice, Industry Canada and Solicitor-General. *Lawful Access – Consultation Document*, Ottawa: August 25, 2002. Available at: http://canada.justice.gc.ca/en/cons/la_al.

Canada. Law Reform Commission. *Electronic Surveillance*. Working Paper #47. Ottawa: 1986.

Canada. Security Intelligence Review Committee. *SIRC Report 2000-2001: An Operational Audit of the Canadian Security Intelligence Service*, Ottawa: 2001. http://www.sirc-csars.gc.ca/

Canada. Solicitor-General. *Annual Report on the Use of Electronic Surveillance 1999*. Ottawa: 2000.

Center for Democracy & Technology, "The Nature and Scope of Governmental Electronic Surveillance Activity," May 8, 2001.

Council of Europe. *Explanatory Report on the Convention on Cybercrime* (ETS No. 185), Strasbourg: November 8, 2001. http://conventions. coe.int/Treaty/en/Reports/Html/185.htm

James Dempsey, "The Carnivore Controversy: Electronic Surveillance and Privacy in the Digital Age," Testimony to the U.S. Senate Judiciary Committee, September 6, 2000. Washington, D.C.: Center for Democracy and Technology, http://www.cdt.org/

----------. "Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy," *Albany Law Journal of Science & Technology*, 8:1 (1997).

Charles Doyle, *The USA Patriot Act: A Legal Analysis,* U.S. Library of Congress. Congressional Research Service. Washington, D.C.: April 15, 2002. RL31377.

Chris Elliott, "The Legality of the Interception of Electronic Communications: A Concise Survey of the Principal Legal Issues and Instruments Under International, European and National Law," Working document for the STOA Panel. European Parliament. Director General for Research, Scientific and Technical Options Assessment programme office, *Development of Surveillance Technology and Risk of Abuse of Economic Information*, vol. 4. Luxembourg: October 1999. PE 168.184/v4

European Commission. *EU Forum on Cybercrime*. "Discussion Paper for expert's Meeting on Retention of Traffic Data," Brussels: 29 October 2001.

European Data Protection Commissioners. *Press Release.* "Statement on Mandatory Systematic Retention of Telecommunication Traffic Data," Cardiff: 11 September 2002.

The European Parliament. Council of the European Union. *The Cyber-Crime Convention*, ETS No. 185, Budapest, Nov. 23, 2001. http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm.

----------.- ----------. *Directive 2002/58/EC*, "Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector," Brussels: 12 July 2002. http://www.gilc.org/as_voted_2nd_read.html

----------. Council of the European Union, *Resolution on the Lawful Interception of Telecommunications,* 17 January 1995 (96/C329/01).

----------. Temporary Committee on the ECHELON Interception System. *Draft Report on the Existence of a Global system for the Interception of Private and Commercial Communications (ECHELON Interception System),* 18 May 2001, PE 305.391.

----------. Director General for Research, Scientific and Technical Options Assessment Programme Office (STOA). *Development of Surveillance Technology and Risk of Abuse of Economic Information*, 5 vols. Luxembourg: Dec. 1999.

European Police Office (EUROPOL). "List of minimum and optional data to be retained by service providers and Telcos," *Questionnaire for Expert Meeting on Cyber Crime: Data Retention*, The Hague, 28 December 2001, File 5121-20020411LR.

Martin L. Friedland, "Police Powers in Bill C-36," in: Ronald Daniels et. al. (eds.), *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill,* Toronto: University of Toronto Press, 2001, pp. 269-85.

Illinois Institute of Technology, IIT Research Institute. *Independent Review of the Carnivore System: Final Report*, Lanham, Md.: 8 December 2000, IITRI CR-030-216, Contract to U.S. Department of Justice.

Donald M. Kerr, "Internet and Data Interception Capabilities Developed by the FBI," *Statement for the record*, U.S. House of Representatives, Committee on the Judiciary, Subcommittee on the Constitution, Washington, DC: 24 July 2000, at: http://www.fbi.gov/congress/congress00/kerr072400.htm

Declan McCullagh, "Will Canada's ISPs become spies?" *CNET News.com*, August 27, 2002.

Gerard McManus, "We dwarf US in phone taps," *Herald Sun* (Melbourne), Sept. 15, 2002.

Stuart Millar and Lucy Ward, "No 10 defends wider electronic surveillance," *The Guardian*, June 12, 2002.

Oliver Moore, "Ottawa Poised to become Big Brother," *Globe and Mail Update*, September 3, 2002, http://rtnews.globetechnology.com/

Richard Norton-Taylor and Stuart Millar, "Privacy fear over plan to store email," *The Guardian*, August 20, 2002.

Kevin Restivo, "Ottawa Mulls Tracking Internet Usage," *National Post*, August 30, 2002.

Jeffrey T. Richelson and Desmond Ball, *The Ties That Bind: Intelligence Cooperation Between the UKUSA Countries*, Boston: Unwin Hyman, 1985.

Shane Schick, "Surveillance may force ISP upgrades," *Communications & Networking*, October 2002.

Lawrence Surtees, "Communication Interception for Security Purposes: CSIS and the Debate on Control," *Canadian Regulatory Reporter*, 4CRR 83, Ottawa: August 1983.

United Kingdom. Secretary of State for the Home Department. *Interception of Communications in the United Kingdom: A Consultation Paper*. London: June 1999.

United States. Department of Justice. Federal Bureau of Investigation. *CALEA Implementation Section. CALEA Flexible Deployment Assistance Guide* (3rd edition). Chantilly, Va.: May 2002. http://www.askcalea.net/

U.S. House of Representatives, Committee on the Judiciary. Testimony of Robert Corn-Revere before the Subcommittee on the Constitution, "The Fourth Amendment and the Internet," Washington, D.C.: April 6, 2000. http://www.house.gov/judiciary/corn0406.htm

U.S. National Security Agency. *United States Signals Intelligence Directive 18*, Fort George Meade: 27 July 1993. (Declassified from Secret). Available from the Federation of American Scientists at http://www.fas.org/

Mark Winther and William Stofega, *The Market for Lawful Intercept Solutions: From the Circuit Switch to Next-Generation Networks and Beyond*, IDC Report #26127, December 2001.

Statutes Cited

Australia. *Telecommunications (Interception) Act*, 1979.

Canada. *Bill C-36,* 49-50 ER II, Nov. 28, 2001

--------. *Criminal Code*, RSC 1985, Chapter C-46

--------. *Canadian Security Intelligence Service Act, (CSIS Act)* Chapter C-23

--------. *National Defence Act,* RSC 1985, Chapter N-5

--------. *Personal Information Protection and Electronics Documents Act (PIPEDA)*, SC 2000, Chapter 5

--------. *Radiocommunications Act*, Chapter R-2

--------. *Security Offences Act*, Chapter S-7

United Kingdom. *Regulation of Investigatory Powers Act (RIPA)*, 2000, chapter 23

--------. *Interception of Communications Act (IOCA)*, 1985

United States. *Communications Assistance for Law Enforcement Act* (*CALEA*), 47 U.S.C., Public Law No. 103-414, 108 Statute 4279.

--------. *The Foreign Intelligence Surveillance Act (FISA)*, 50 U.S.C., Public Law No. 95-511.

--------. *Omnibus Crime Control and Safe Streets Act,* 18 U.S.C., Public Law No. 90-351, Title III, 82 Statute 212 (codified as amended at 18 U.S.C. 2510-2522 (1996).

--------. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* (*USA PATRIOT Act*), Public Law No. 107-56, 115 Statutes 272, October 26, 2001.

Legal Cases

Supreme Court of Canada

Mario Duarte v. Her Majesty the Queen (1990), 1 SCR 30 Canada. File No. 20542.

Hunter v. Southam (1984), 14 CCC (3d) 97 (SCC)

R. v. Plant (1993) 3 SCR 281

United States Supreme Court

Smith v. Maryland, 442 U.S. 735, 742 (1979).

Appendix 1: Law Enforcement Traffic Data Retention 'Wish List'

Table 2
Proposed EUROPOL Traffic Data Retention Requirements for Internet Service Providers

Technical Element	Minimum Data Requirement	Optional Data Requirement
Network Access Systems - Access logs for authentication servers and IP routers	Date and time of connection to server	User credit card no.
	User ID and password	Bank account info for monthly payment
	Assigned IP and storage addresses	
	Number of bytes transmitted and received	
	Caller Line Identification (CLI)	
Email Servers - SMTP	Date and time of connection to server	
	IP address of sending computer	
	Message ID (msgid)	
	Sender (login@domain)	
	Receiver (login@domain)	
	Status indicator	
Email Servers - Post office protocol or IMAP logs	Date and time of connection to server	
	IP address of client	
	User ID and password	
File Upload/Download servers - FTP Log	Date and time of connection to server	
	IP source address	
	User ID and password	
	Path and filename of data object	
Web Servers - HTTP Log	Date and time of connection to server	Last visited page
	IP source address	Response codes
	Operation	
	Path of operation to retrieve html page	
	Web page update details	
Usenet - Network News Transfer Protocol (NNTP) logs	Date and time of connection to server	
	Protocol process ID	
	Hostname; DNS name of IP address	
	Basic client activity (without content)	
	Posted message ID	

Table 2
Proposed EUROPOL Traffic Data Retention Requirements for Internet Service Providers

Technical Element	Minimum Data Requirement	Optional Data Requirement
Internet Relay Chat - IRC log	Date and time of connection to server	Copy of contract
	Session duration	Bank account/credit card info
	Nickname used during IRC connection	
	Hostname and/or IP address	

Source: EUROPOL "List of minimum and optional data to be retained by service providers and Telcos," *Questionnaire for Expert Meeting on Cyber Crime: Data Retention*, The Hague, 28 December 2001, File 5121-20020411LR; IDC Canada, 2002

Table 3
Proposed EUROPOL Traffic Data Retention Requirements for Wireline Telecom Carriers

Minimum Data Requirement	Optional Data Requirement
Called number - even if call unsuccessful	Copy of contract
Calling number - even if call unsuccessful	Nature of telecommunication (voice, modem, fax, etc)
Date and time of start and end of call	
Type of call (incoming, outgoing, link)	
Intermediate conference numbers	
Name, DOB, address of subscriber	
Billing address	
Start and end dates of service	
Type of connection	
Forwarded called number	
Time span	
Means of payment	

Source: EUROPOL "List of minimum and optional data to be retained by service providers and Telcos," *Questionnaire for Expert Meeting on Cyber Crime: Data Retention*, The Hague, 28 December 2001, File 5121-20020411LR; IDC Canada, 2002

Table 4
Proposed EUROPOL Traffic Data Retention Requirements for Wireless Operators

Minimum Data Requirement	Optional Data Requirement
Called number - even if call unsuccessful	Copy of contract
Calling number - even if call unsuccessful	Nature of telecommunication (voice, modem, fax, etc)
Date and time of start and end of call	
Type of call (incoming, outgoing, link)	
Intermediate conference numbers	
Name, DOB, address of subscriber	
Billing address	

Table 4
Proposed EUROPOL Traffic Data Retention Requirements for Wireless Operators

Minimum Data Requirement	Optional Data Requirement
Called number - even if call unsuccessful	Copy of contract
IMSI and IMEI numbers	
Start and end dates of service	
Device identification	
Identification and geographical location of cell sites used	
Ground station location	
WAP service details	
SMS (date and time, incoming or outgoing; telephone number	
For IP-based wireless services, all other data retained for IP address	

Source: EUROPOL "List of minimum and optional data to be retained by service providers and Telcos," *Questionnaire for Expert Meeting on Cyber Crime: Data Retention*, The Hague, 28 December 2001, File 5121-20020411LR; IDC Canada, 2002

Appendix 2: *CALEA* J-Standard Intercept Features & FBI 'Punchlist'[63]

The Telecommunications Industry Association (TIA) developed the J-STD-025 *Lawfully Authorized Electronic Surveillance (LAES)* technical standard, commonly known as the J-Standard, in response to *CALEA* requirements. A trade association based in Arlington, Virginia, the TIA represents both telecommunications service providers and equipment vendors throughout North America.

The J-Standard specifies the technical aspects of the ability to collect call-identifying information and call content information from wireline, cellular, and broadband personal communications services (PCS) carriers. It defines the intercept function in five broad categories: access, delivery, collection, service provider administration, and law enforcement administration:

- The Access Function consists of one or more intercept access points (IAPs). These IAPs provide access to an intercept subject's communications, call-identifying information, or both.

[63] This appendix is based on: Mark Winther and William Stofega, *The Market for Lawful Intercept Solutions: From the Circuit Switch to Next-Generation Networks and Beyond*, IDC Report #26127, December 2001; and: United States. Department of Justice. Federal Bureau of Investigation. *CALEA Implementation Section. CALEA Flexible Deployment Assistance Guide* (3rd edition). Chantilly, Va.: May 2002. http://www.askcalea.net/

- The Delivery Function is responsible for delivering intercepted communications and call-identifying information to one or more collection functions (i.e., monitoring equipment at law enforcement locations). The delivery function delivers information over two distinct types of channels: Call Content Channels (CCCs) and Call Data Channels (CDCs). The CCCs are generally used to transport call content, such as voice or data communications. The CDCs are generally used to transport messages that report call-identifying information, such as calling-party identities and called-party identities.
- The Collection Function is responsible for collecting and recording lawfully authorized intercepted communications (e.g., call content) and call-identifying information for law enforcement agencies (LEAs). The collection function is the responsibility of law enforcement.
- The Service Provider Administration Function is responsible for controlling the surveillance functions within the carrier network.
- The Law Enforcement Administration Function is responsible for controlling the surveillance and collection functions within the law enforcement site.

The basic features of the J-Standard include:

- ***CALEA* basic surveillance.** Provides support for basic surveillance on plain old telephone service (POTS), business, centrex, and ISDN Basic Rate Interface (BRI) lines.
- **Redirection interception.** Provides support for the interception of communications on forwarded calls controlled by the subject (party under surveillance as identified in a court order).
- **Call content delivery.** Provides support for the use of standard digital trunks as the circuits that deliver call content to the monitoring center.
- **Call data delivery.** Provides support for the delivery of call data messages over an ethernet facility using TCP/IP protocols.
- ***CALEA* administrative interface.** Provides a secure password-protected level accessible via a standard teletype (TTY) interface.
- **J-STD-025 call data message set.** Provides for the generation and delivery of call data messages over the CDC interface.
- **Feature interaction.** Provides interworking with a subset of commonly deployed digital multiplex system

(DMS) features (e.g., Call Waiting, Three-Way Calling, Advanced Intelligent Network E800, and Local Number Portability).

In addition to those monitoring capabilities outlined in the J-Standard, the U.S. Federal Communications Commission has also reaffirmed its 1999 decision that certain other specific surveillance capabilities sought by the FBI should be built into telephone switches. Those added features, known as the "punchlist," include the ability to extract digits dialed by a subject after the initial call setup is completed and the ability to provide information identifying parties as they join or drop off a conference call. The punchlist includes nine other required *CALEA* functions for future implementation:

- Conference call monitoring. This capability allows the continued monitoring of subject-initiated conference call content, including the call content of parties on hold.
- Party hold, join, drop on conference calls. This identifies the active parties on a call, including whether a party is on hold, has joined, or has been dropped from the conference call.
- Subject-initiated dialing and signaling information. This provides access to the subject's use of feature keys (e.g., call forwarding, call waiting, call hold, and three-way calling).
- In-band and out-of-band signaling. This enhancement adds all signaling sent to the subscriber's or an associate's phone (such as ringing, busy signals, call waiting tones) not previously carried by the call data channel.
- Timing information. This enhancement reports call timing information to the monitoring center to correlate call-identifying information with the call content of a communications interception.
- Dialed digit extraction. With this capability, all digits dialed by the subject after the initial call setup is completed (e.g., personal identification numbers [PINs], credit card numbers) are collected and sent to the monitoring center.
- Surveillance status message. This verifies to a LEA that a wiretap had been established and was functioning correctly.
- Continuity check tone. This alerts a LEA if the facility used for delivery of call content interception failed or lost continuity.
- Feature status message. This notifies a LEA that, for the subject under surveillance, specific subscription-based services were added or deleted.

The FCC adopted the first six items and made the last three items optional at the carrier's discretion. Four of those six items were reaffirmed by the FCC on April 11, 2002 following an appeal, with compliance ordered by June 30, 2002.

The existing telecommunications intercept standards (J-Standard in the United States and ETSI in Europe) still face significant regulatory and technical problems when applied to packet networks, including:

- Interception access points. There are multiple potential access points necessary to achieve full intercept capability in packetized voice networks. IAP considerations include network components (media gateways, routers, softswitches, application servers) and traffic flow (local, national, international transit, and origination and termination networks).
- Packets travel in different directions. Real-time transport protocol (RTP) sessions (or call bearer channels) may go via one route while Media Gateway Control Protocol (MGCP) or Session Initiation Protocol (SIP) sessions (call data traffic) may go another route. Customer premise equipment may also have two or more links to the network.
- Emergence of SIP clients. The new Windows XP operating system software from Microsoft includes SIP client software that enables any Windows XP-equipped PC to make a phone call. Will this be subject to lawful intercept requirements, and will it be feasible to do wiretaps on those clients?
- *CALEA*/ETSI feature challenges. Features that are relatively easy to provide in circuit-switched environments, such as call forwarding and dialed digit extraction, are more difficult in a softswitch environment.
- Encryption. Most governments have initiatives underway to control encryption technologies. However, it is likely that encryption will proliferate in a packet environment, creating greater challenges for intercept.
- Compression. Like encryption, different types of compression schemes are available in a packet voice environment, including numerous codec CPE alternatives. With no regulation of codec types, lawful intercept compliance will require identifying and supporting many codec types.
- Vulnerabilities. To the extent that packet voice networks comply with lawful intercept requirements, they also become more vulnerable to illegal wiretaps.

Appendix 3: U.S. National Security Rules for Intercept Retention[64]

Electronic surveillance is conducted by elements of the Intelligence Community for foreign intelligence and foreign counterintelligence purposes. Such surveillance is subject to regulation by statute, by Executive Order No. 12333 and agency directives governing the collection, retention, or dissemination of information concerning U.S. persons.

Communications interception activities of the U.S. National Security Agency are governed by *Department of Defense Directive 5240.1-R*, "DoD Activities that May Affect U.S. Persons." Those guidelines are expanded on in an internal NSA directive, *U.S. Signals Intelligence Directive 18*, whose provision on intercept retention is excerpted below:

SECTION 6 - RETENTION

6.1 (S-CCO) Retention of Communications to, from or About U.S. PERSONS.

a. Except as otherwise provided . . . communications to, from or about U.S. persons that are intercepted by the USSS [United States SIGINT System] may be retained in their original or transcribed form only as follows:

(1) **Unenciphered communications not thought to contain secret meaning may be retained for *five years*** unless the DDO determines in writing that retention for a longer period is required to respond to authorized FOREIGN INTELLIGENCE requirements.

(2) Communications necessary to maintain technical data bases for cryptanalytic or traffic analytic purposes may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future FOREIGN INTELLIGENCE requirement. ***Sufficient duration may vary with the nature of the exploitation and may consist of any period of time*** during which the technical database is subject to, or of use in, cryptanalysis. If a U.S. person's identity is not necessary to maintaining technical databases, it should be deleted or replaced by a generic term when practicable.

---

[64] U.S. National Security Agency. *United States Signals Intelligence Directive 18*, Fort George Meade: 27 July 1993. (Declassified from Secret). [Emphasis added.] Available from the Federation of American Scientists at http://www.fas.org/

IDC
Analyze the Future

IDC Canada
36 Toronto Street, Suite 950
Toronto, Ontario M5C 2C5
Tel: 416/369-0033
Fax: 416/369-4019

For more information, contact:
Lawrence Surtees
Director, Telecommunications and Internet Research, IDC Canada
Phone: 416/369-0033 ext. 297
E-Mail: lsurtees@idccanada.com

Megan Branch
Manager, Marketing and Business Development, IDC Canada
Phone: 416/369-0033 ext. 272
E-mail : mbranch@idccanada.com

Privacy Through Your Service Provider a Thing of the Past, says IDC

TORONTO, October 29, 2002 - Ottawa is looking to capture much more than your tax dollars and census stats. According to a recently released IDC report, Ottawa's commitment to the first international Cyber-crime treaty will have a major impact on private citizens, corporations, and Internet-industry players. The European Union treaty provides legal tools which preserve select communications traffic information in order to assist in the investigation and prosecution of computer crime. Such tools however would require online surveillance, including Web surfing and email history, for all Internet users in Canada.

IDC examines this issue beyond the public concern for privacy to the Internet-industry players. The study offers highly valuable guidance on the issues and questions service providers in Canada need to consider in drafting their comments on the federal government's "Lawful Access" proposal to implement the treaty. Lawrence Surtees, Director of Telecommunications and Internet-related Research for IDC Canada advises, "The industry is alarmed by the considerable cost issue, likelihood of soaring storage requirements, and the sheer scale of the impact the adoption of these legal tools would have. Service providers must have a solid understanding of all the factors that the treaty proposals will carry before they can begin to calculate the cost to their business."

The proposed legal changes would require all telecommunications and Internet service providers to build automatic real-time surveillance capabilities into all their networks and create a national database of all Internet users. Companies that provide Internet, wireline and wireless services would be required to collect and maintain content and telecommunications-associated specific data. The collection and retention of such vast amounts of data is hugely complex and problematic for service providers. IDC's study assists to clarify the proposal and outline the real issues at hand for clients.

Although the changes could bolster powers to fight crime and terrorism, they would weaken privacy for Internet users and cause financial strife for service providers, the cost of which may in turn be passed on to individual service customers. IDC's study of the treaty and it's effects on the industry will enable service providers to begin to formulate their business strategies as they grapple with the impact this major issue will have on the future of their organizations and the IT industry in Canada.

About IDC

IDC is the foremost global market intelligence and advisory firm helping clients gain insight into technology and ebusiness trends to develop sound business strategies. Using a combination of rigorous primary research, in-depth analysis, and client interaction, IDC forecasts worldwide markets and trends to deliver dependable service and client advice. More than 700 analysts in 43 countries provide global research with local content. IDC's customers comprise the world's leading IT suppliers, IT organizations, ebusiness companies and the financial community. Additional information can be found at www.idc.com.

IDC is a division of IDG, the world's leading IT media, research and exposition company.

###