Department of Justice Canada
Ministère de la Justice Canada

# SUMMARY OF SUBMISSIONS TO THE LAWFUL ACCESS CONSULTATION

**Nevis Consulting Group Inc.**
**General Editor**

**April 28, 2003**

Canada

# CONTENTS

# CHAPTER 1: INTRODUCTION

## A. BACKGROUND

Interception of communications and search and seizure of information have proved to be effective law enforcement tools for police and national security agencies throughout the developed world. The same is true in Canada, where these activities are carried out mainly by police forces and CSIS[1] under legal authority provided in the *Criminal Code* and the *Canadian Security Intelligence Service Act*. In cases where lawful interception evidence was presented to the courts in 2000, over 90% resulted in conviction of the accused[2].

Lawful interception used to be relatively straightforward when most of the world's telecommunications consisted of voice conversations which were carried over wireline networks operated by a small number of large telephone companies. Much of Canada's legislation dealing with lawful access[3] was introduced during this era. The arrival of telecommunications industry deregulation, the Internet, cellphones, wireless e-mail, high speed fiber-optic networks and VoIP[4] has changed the picture considerably. Law enforcement agencies[5] find that these more advanced services present technical and legal challenges to conventional lawful access methods and that the provisions of existing legislation are inadequate to sustain effective interception capability across the network. Meanwhile, criminal elements are using communications facilities that cannot be readily intercepted by Canadian law enforcement and national security agencies, even though the agencies have lawful authority to do so.

The need to update Canada's lawful access legislation is also being driven by international obligations in the struggle against global crime. Canada has signed the Council of Europe's *Convention on Cybercrime* which is designed to help equip signatory states with legal tools to assist in the investigation and prosecution of computer crime, including Internet-based crime and crime involving electronic evidence. The *Convention* also calls for increased international cooperation in tackling cybercrime and for increased commonality in the legislation available in each country to prosecute it. Before Canada can ratify the *Convention,* the *Criminal Code* will need modification to include provision for production orders, preservation orders and offences relating to computer viruses and similar devices.

As part of the process to update Canada's lawful access legislation, the Department of Justice, the Portfolio of the Solicitor General[6] and Industry Canada reviewed a variety of options to address the difficulties presented to lawful access by modern communications technologies. A formal consultation process was then launched with industry, civil society groups[7], law enforcement, privacy

---

[1] Canadian Security Intelligence Service.

[2] Solicitor General's *Annual Report on the Use of Electronic Surveillance*, *2000* - www.sgc.gc.ca/policing/publications_e.asp.

[3] Interception by law enforcement and national security agencies and search and seizure by law enforcement agencies.

[4] Voice over Internet Protocol.

[5] References to "law enforcement" or "law enforcement agencies" in this report may be taken to mean "law enforcement and national security agencies" except where the context clearly indicates otherwise.

[6] Portfolio of the Solicitor General refers to the Department of the Solicitor General of Canada, Royal Canadian Mounted Police (RCMP) and Canadian Security Intelligence Service (CSIS).

[7] For the purposes of this report, civil society groups comprise civil liberty associations, community groups, consumer representatives, non-governmental privacy/freedom of information organizations and associations representing the legal profession. Participating governmental privacy and information commissioners are shown separately in Annex C.

and information commissioners and the general public to seek their views on the issues involved.

A paper entitled the *Lawful Access Consultation Document* was released in August 2002 to provide a basis for the consultation and to encourage input on a range of proposals geared to modernize Canada's lawful access legislative framework. This paper is available online at the Department of Justice website located at www.Canada.justice.gc.ca/en/cons/la_al .

"The public policy objectives of the process are to maintain lawful access capabilities for law enforcement and national security agencies in the face of new technologies and to preserve and protect the privacy and other rights and freedoms of all people in Canada".

*Lawful Access Consultation Document* [8]

## B. The Nature of this Report

This report provides a summary of the written submissions from law enforcement, companies, organizations and the public in response to the proposals presented in the consultation document. The response has been substantial and wide-ranging in content. It has provided a wealth of useful suggestions on how the proposals in the consultation document could be improved, expanded or discarded. There were responses expressing sincere concern, some making detailed legal arguments, while others were notable for their robust and candid remarks.

Practically all submissions contained observations that deserve a place in this report. Unfortunately, it is only possible to include a representative sample of what people said. This task has been made easier, however, by the consistency of views expressed by respondents in each group on a number of key issues.

The report consists of an introduction which outlines the reason for the lawful access consultation and describes the consultation process. An overview of the responses is provided for those who want a quick appreciation of the opinions put forward. This consists of ten observations from each group of participants - law enforcement, industry, privacy and information commissioners, civil society groups and the general public, selected on the basis of the frequency with which they were expressed by respondents.

A more detailed account of the comments received from each of these groups follows, broadly arranged under the same headings as those in the consultation document. In the event that there were no comments relating to a given topic by a particular group, that heading is not included.

## C. The Consultation Process

As mentioned previously, Canadians were given the opportunity to consider lawful access issues and options for change based on the consultation document. The consultation period began in August 2002 with an initial closing date for submissions of November 15, 2002. This date was subsequently extended until December 16, 2002 in response to written requests from several interested parties.

In addition, the consultation process included a series of more than 20 meetings between key stakeholders and the government departments involved[9]. These allowed participants to obtain a closer understanding of the government's objectives before preparing their formal responses and to seek clarification on issues important to their areas of interest. Participants included law enforcement

[8] Page 6.

[9] Department of Justice, the Portfolio of the Solicitor General of Canada and Industry Canada.

agencies, industry associations and companies, privacy and civil liberties organizations, the Privacy Commissioner of Canada and provincial governments. The general public was encouraged to respond to the consultation document via e-mail and regular post.

## D. RESPONSE FROM CANADIANS

Law enforcement's contribution focused on a comprehensive paper submitted by the Canadian Association of Chiefs of Police (CACP) which was supported by written communications from 55 police forces, including numerous RCMP detachments from across Canada. A small number of police forces provided additional comments based on their regional experience.

Industry contributed 19 responses from companies involved in the telecommunications business and from related business associations, while five of Canada's privacy and information commissioners provided their views.

A total of 14 civil society groups delivered submissions that concentrated on privacy and other human rights issues. Two of the organizations are based in the US and were able to offer views based on their experience with similar legislation passed by Congress in recent years.

Responses were received from 219 individuals - almost all Canadians[10]. Most arrived by e-mail and ranged from adamant opposition to the proposals to warm support for the consultation process. Ontario contributed about 50% of these submissions, BC and Alberta 38% and Quebec 7%. Approximately 2% were from women.

[10] A number of responses were anonymous or without indication of the sender's location, so it is not possible to be sure of the actual Canadian content.

# CHAPTER 2: RESPONSE OVERVIEW

## 2.1 LAW ENFORCEMENT

1. Police services expressed strong support overall for the proposals.

2. The ability of police to lawfully access telecommunications services has not kept up with the advances in communications technology. This gap is creating a safe zone where criminals can communicate free from fear of detection. It must be technically possible for police to lawfully intercept all telecommunications services offered in Canada without exception.

3. Communications Service Providers (CSPs)[11] should pay for installing lawful access capability on new or significantly upgraded services. The government should specifically prohibit CSPs from directly or indirectly recovering infrastructure costs from law enforcement agencies through any cost recovery scheme, such as burying them in operational or hook-up charges.

4. In principle, CSPs should be able to recover reasonable costs of providing operational assistance to law enforcement. These costs should be distributed over a broad base (like the existing 911 fee) rather than being recovered from individual police services. However, CSPs must not be permitted to impose fees or other charges as a condition of compliance with a judicial order.

5. A compliance mechanism that is independent of government should be established in order to determine conformity with the legislation.

6. Forbearance of interception capability and capacity should be the exception rather than the rule. CSPs should be required to submit an implementation plan with each forbearance application, with quarterly reporting, showing in detail how full compliance with the legislation will be achieved.

7. Significant fines should be imposed on CSPs for non-compliance with mandatory capability requirements. With law enforcement and service providers working together in a cooperative partnership, the vast majority of difficulties will be worked out. Only the most severe and blatant contraventions of the capability and capacity standards set out in the proposed legislation would result in enforcement action.

8. Lawful interception of private communications by police in Canada must continue to be subject to prior court approval.

9. CNA and LSPID[12] is not personal information and law enforcement agencies should not need a judicial authorization to obtain it. A statutory provision should be created requiring CSPs to provide law enforcement and national security agencies with CNA and LSPID information. If this is rejected on privacy grounds, a production order with a nominal procedural threshold should be considered instead.

10. To help combat increasing international crime, Canadian lawful access powers need to be harmonized with those available in other countries. Australia, the Netherlands, New Zealand, the United Kingdom and the United States are ahead of Canada in adopting lawful access legislation in line with today's technology.

[11] The second text box on page 20 shows the types of service provider grouped as CSPs in this report.
[12] CNA - Customer Name and Address, LSPID - Local Service Provider Identification.

## 2.2 INDUSTRY

1. Most CSPs who responded were supportive of the need for effective lawful access in the face of technological change[13].

2. The consultation document lacks detail and is too imprecise to allow anything but high-level comments. Further consultation is called for, including the opportunity to comment on the specific proposals contained in draft legislation and accompanying regulations, prior to their introduction in Parliament.

3. The interception of unviewed e-mail and similar digital communications traffic in transit should be considered interception of a "private communication" and therefore subject to the protections contained in a *Criminal Code* Part VI authorization. A search warrant or production order should be required for law enforcement to access opened e-mail that a user has chosen to retain.

4. The circumstances under which a forbearance order may be justified should be stated, as well as the criteria that will be used to evaluate when, and for how long, such orders will be valid. Any rules or standards dealing with the forbearance power should be clear and transparent.

5. The legislation should ensure that law enforcement agencies remain responsible for reasonable costs incurred by service providers making operational assistance available to law enforcement agencies in carrying out lawful interception, seizure and preservation orders. These costs should be worked out between each service provider and the agency concerned rather than being based on universal tariffs laid out in the regulations for various types of support. Industry Canada and the Solicitor General, or an independent arbitrator, should mediate any disputes about fees for service between a CSP and a law enforcement agency.

6. Definitions provided in the consultation document differ from those given in the *Telecommunications Act*. Some important terms such as "basic intercept capability" are not defined. Clear consistent definitions in line with those used internationally are essential to the success of the proposed legislation.

7. The government should pay for the "basic intercept capability" until lawful access solutions are readily available for the transmission equipment used by service providers that can be deployed and maintained at minimal incremental cost to the service provider. This is regardless of how "significant upgrade" and "new service or technology" are defined in the resulting legislation.

8. The consultation document failed to show that the current provisions in law are inadequate to allow effective access to data communications services in Canada or that investigations or prosecutions have been unsuccessful due to lack of technical capability.

9. There is strong opposition against obliging service providers to collect, maintain or guarantee the accuracy of subscriber information beyond that needed for their own business purposes.

10. CSPs are also strongly opposed to the creation of a national CNA/LSPID database, citing privacy and security concerns as well as the high costs of developing and maintaining such a database. They point out that most cybercriminals are quite capable of using false names, hacked accounts or public access terminals to communicate or transact.

[13] The others did not express a view on the matter.

### 2.3 PRIVACY AND INFORMATION COMMISSIONERS

1. The consultation document does not demonstrate why the proposed measures are necessary.

2. New technologies and communications services may well pose a challenge to existing interception methods and require CSPs to provide law enforcement agencies with basic interception and surveillance capabilities to achieve lawful access to them.

3. The proposed measures go far beyond what is necessary to maintain existing capabilities and authorities in the face of modern communications technology.

4. E-mails should not be subject to a lower standard of protection than telephone calls or letters. In the same way, Internet browsing should not be afforded less protection than book purchasing or researching in a reference library.

5. Canadians are entitled to feel confident that their communications and on-line activities will not be arbitrarily intercepted or scrutinized.

6. If the *Convention on Cybercrime* calls for unjustifiable intrusion on the privacy rights of Canadians which is inconsistent with our values and rights, the *Convention* should not be ratified by the Canadian government.

7. The government should continue to resist any suggestions that general data *retention* requirements be part of the lawful access initiative.

8. A national database for CNA/LSPID information should not be created. There is no need to change the current law and practice concerning access to this information.

9. An obligation on those selling pre-paid cellphones or phone cards to collect people's sensitive information such as driver's license and credit card numbers before making the sale would be a gross invasion of privacy.

10. Nowhere does the consultation document indicate that accountability measures are being contemplated.

### 2.4 Civil Society Groups

1. The consultation document is unclear about the government of Canada's proposals.

2. The draft legislation and accompanying regulations should be made available for full and complete public review with sufficient time for interested parties to assess their impact and submit comments.

3. The document is unconvincing on how the proposals would actually help fight organized crime or terrorism. The government will no doubt have more access to the private lives of Canadians, but serious criminals and terrorists are unlikely to be careless enough to fall within the scope of the proposed measures.

4. If evidence is available to justify the proposed legislative amendments, it should be made public so that it can be seen whether the security benefits outweigh the privacy costs. If such evidence does not exist, the measures should be dropped.

5. The proposals would establish a lower standard for lawful interception and/or search and seizure of online communications versus telephone and postal mail, for example. No justification has been provided for this. *Criminal Code* standards should be designed to apply regardless of technology.

6. Any new legislation should specifically address privacy issues wherever individual privacy is at risk. General references to the *Canadian Charter of Rights and Freedoms* (the *Charter*) and the *Personal Information Protection and Electronic Documents Act (PIPEDA)* are insufficient.

7. The government has failed to present evidence that this massive surveillance infrastructure is necessary. For example, it is unknown how many investigations have actually been seriously hampered by lack of technical capability.

8. If law enforcement agencies have difficulty in dealing with new communications technologies, the solution is not to lower legal standards for interception, but to provide law enforcement agencies with the technical expertise and equipment they need to deal with the evolving environment.

9. The proposals require customers or their CSPs to pay for the surveillance. This is wrong in principle and impracticable in operation.

10. The job of ISPs is to provide services for their customers. This should not include monitoring those customers for the purposes of the state. Production orders must not be used to circumvent the high thresholds that would be required if law enforcement agencies were carrying out the search or interception themselves.

## 2.5 GENERAL PUBLIC

1. The opportunity to comment on these proposals is much appreciated.

2. It is not clear what benefit is to be gained from the proposed legislative changes that does not already exist in the law today.

3. It is a matter of serious concern when international treaties such as the *Convention on Cybercrime* are signed without democratic consultation and then presented to the public as though it is essential that they be ratified.

4. The consultation document fails to show how the Internet has "created difficulties for investigators". Also, in the case of the Internet, the "need for sophisticated equipment" seems to boil down to packet sniffers which are widely used by ISPs and available for a few thousand dollars each.

5. No case is made in the consultation document that Canadians deserve less privacy when using digital communication rather than analog electronics, or indeed when they use electronics rather than pen and ink.

6. Data encryption is widely used by criminals and terrorists when communicating over private and public networks including the Internet. Encryption techniques are often not detectable, not interceptable and can render law enforcement and CSP interception technology ineffective.

7. Should a law enforcement agency require assistance from a service provider that is beyond the normal cost of doing business for that provider, then the agency should pay the cost of the assistance. Such costs should not be the responsibility of the service provider nor should they be passed on to the end client.

8. No CSP should be an information collection agency on behalf of the Canadian government. If the government wants and needs information, it should be responsible for retrieving, collecting and storing it. The CSP should only be obliged to provide the facilities when there is a lawful order to do so.

9. Another national database of personal records is completely unnecessary. There is no national registry of telephone users or postal mail users - there should not be one for Internet users. A national database of this kind would also be a dangerous accumulation. Can bureaucrats guarantee that this highly sensitive database would never be successfully hacked?

10. E-mails should require a court order for interception regardless of the point of interception.

# CHAPTER 3: COMMENTS BY LAW ENFORCEMENT

**Total Number of Written Submissions Received: 58**

The Canadian Association of Chiefs of Police submitted a response to the lawful access consultation document on behalf of Canadian law enforcement[14]. The majority of individual police forces wrote separate letters indicating their support for the CACP submission. A number of RCMP detachments also responded expressing support for the lawful access initiative. Several police forces had additional points to make that have been included in the summary below. Due to their subject matter, submissions from two government departments have also been included in this chapter. A list of law enforcement respondents is given in Annex A and the government departments are shown in Annex E.

## A. GENERAL

1. Communications technology has continued to advance rapidly but the ability of police to access telecommunications services and gather necessary information to apprehend criminals has not. This gap is creating a safe zone where serious criminals can operate free from fear of detection and arrest.

2. Canadian law enforcement considers a number of broad principles to be very important to this discussion:

- The circumstances in which Canadian police may intercept private communications must continue to be the subject of prior court approval.

- The technological ability to implement court ordered access must always exist and never be compromised. There should be no "intercept safe havens"[15] in Canada.

- New communications technologies are not of themselves problematic. However, left unregulated and without the necessary checks and balances, they can have unintended detrimental consequences. Modern legal mechanisms are required to ensure we as a society balance the needs of global competitiveness with those of effective public safety.

- Modern communications technology shrinks distances and operates free of geographical constraints. Organized criminals, Internet predators and terrorists take advantage of these facts. Legislation in Canada must reflect the growth of cross border crime.

- Some service providers require law enforcement agencies to pay significant fees before they will implement a court ordered interception. No persons, whether corporate or otherwise, must be permitted to erode the authority of the court by imposing fees or other financial obligations as a condition of compliance with a lawful order from the court.

---

[14] Prepared by the Law Amendments Committee of the CACP and the Lawfully Authorized Electronic Surveillance (LAES) Sub-Committee. LAES is a standing group of experts in the field of lawful access with representatives from federal, provincial and municipal law enforcement, as well as national security agencies.

[15] CACP defines Intercept Safe Haven as: "Any technology, application or device that when used as a means of communication, by its design or through its use in conjunction with other technologies, applications or devices, either intentionally or unintentionally, impedes, hampers or otherwise does not allow for the identification of or the interception of the communication".

3. High speed Internet and modern wireless services benefit Canadians at large. At the same time, police are increasingly faced by sophisticated criminals who use these same telecommunications technologies to support their unlawful operations and to hinder police efforts to bring them to justice.

4. Canadian lawful access powers need to be harmonized with those available in other countries, to help combat increasing international crime. Australia, New Zealand, the United Kingdom, the Netherlands and the United States are ahead of Canada in adopting lawful access legislation in line with today's technology.

5. Lawful access provisions should be transparent. That is, they should clearly articulate the appropriate procedure to be followed depending on the type of evidence and the expectation of privacy attached to it. They should also be transparent in the sense that they are framed in as technology neutral terms as possible.

**B. REQUIREMENTS TO ENSURE INTERCEPT CAPABILITY**

1. The minimum acceptable standard is that all new or significantly upgraded services shall be intercept capable, with the goal that all telecommunications services operating in Canada shall be intercept capable within a specific period of time defined in the legislation.

2. CSPs should have the technical capacity to provide real-time access for law enforcement and national security agencies to the following information and services, regardless of the range of services and features offered to the subscriber:

1. The telecommunications of the subject of an interception order isolated from any telecommunications outside the scope of the order and to provide the intercepted information only to the specified law enforcement or national security agency.

2. The entire telecommunications of the subject, including content, allowing the authorized agency to conduct real-time monitoring for the full duration of the interception.

3. All attempts of the subject to establish telecommunications.

4. A means to accurately associate the telecommunications associated data[16] with the call content.

5. The physical, personnel and administrative measures to ensure security in relation to interceptions.

6. Telecommunications encrypted by the CSP to be delivered to authorized agencies *en clair*.

7. The transmission to law enforcement and national security agencies of the most accurate location information available to the CSP network.

**C. REGULATIONS**

1. Regulations should not only be consistent with international standards, but should also be effective and workable in Canada.

[16] Means the same as "traffic data" and "associated traffic data" in this report.

2. Regulations will be required to allow law enforcement agencies to access both the content of communications and the related traffic data such that they may be associated together to an acceptable standard for use as evidence in criminal proceedings.

3. CSPs must be required to enable police to monitor only those targets authorized in a given court order. This would include obligations to ensure the privacy and security of the content of the intercepted communication, the associated traffic data and the identities of related persons.

4. Regulations should define the required capacity for simultaneous interception at service provider facilities, security requirements for police operations, as well as the integrity, competence and reliability of the service provider staff involved.

5. Regulations should prohibit CSPs from recovery of infrastructure costs from law enforcement and national security agencies through any cost recovery scheme - such as burying them in operational or hook-up charges.

**D. FORBEARANCE**

1. Forbearance of intercept capability and capacity obligations should be the rare exception rather than the rule.

2. Disputes between law enforcement agencies and CSPs as well as forbearance requests should be handled either by an arm's length body responsible to the Solicitor General and the Minister of Industry or by a cabinet appointed three person board with representatives from the federal Solicitor General's office, Industry Canada and the CACP Lawfully Authorized Electronic Surveillance (LAES) subcommittee.

3. Forbearance sections in the proposed legislation should cease to operate and no further applications for forbearance should be accepted five years after the legislation receives Royal Assent.

4. Forbearance applications should be processed within 90 days from receipt and applicants should not be subject to the financial or other penalties set out in the legislation during this period.

5. Forbearance should not be granted for intercept capabilities 1, 2, 3, 4 and 6 listed in B2 above or if the forbearance might result in the creation of an "intercept safe haven".

6. CSPs should be required to submit with each forbearance application an implementation plan, with quarterly reporting, showing in detail how full compliance with the legislation will be achieved. The period granted for a given forbearance should not exceed 12 months. At the end of this time, the CSP should either be fully compliant or should be required to apply for a 12 month extension which would be assessed as a new application.

**E. COMPLIANCE MECHANISM**

1. A compliance mechanism should be put in place by the proposed legislation which is independent of government, effective, efficient, appropriately funded and resourced. It should also be responsible for forbearance decision-making with appeals being made to the federal cabinet (see D2 above).

2. Significant fines should be imposed for non-compliance with mandatory capability requirements.[17]

[17] CACP reports that fines in Australia range up to A$10 million for companies in the case of serious and blatant breaches of capability standards.

3. With law enforcement and service providers working together in a cooperative partnership, the vast majority of difficulties will be worked out. Only the most severe and blatant contraventions of the capability and capacity standards set out in the proposed legislation would result in enforcement action.

**F. COSTS**

1. CSPs should bear the entire cost of providing access capability to new or significantly upgraded technologies.

2. Even when the capability to intercept exists and the courts have authorized the interception, some CSPs have attempted to impose significant charges on the police - leading to regrettable ad hoc agreements between law enforcement agencies and individual telecommunications companies. Canadian law enforcement maintains that these costs relate to the public good and urges the government to legislate a firm prohibition against CSPs charging fees for compliance with any court orders. CSPs should also be prevented from recovering infrastructure costs[18] from police forces.

3. Some CSPs charge law enforcement agencies look-up charges for subscriber information which is provided free of charge to the public - such as access to the Local Service Provider Identification (LSPID) database on the web. There seems little or no justification for this practice. Any charges for more demanding look-up tasks, such as subject telecommunications history, should take into account how readily CSPs can access the required information given fast access to in-house databases and other up-to-date facilities.

4. Haulback lines to transfer intercepted material from the CSP to police and national security agency facilities are charged by Canadian carriers at commercial rates, in line with Canadian Radio-television and Telecommunications Commission (CRTC) regulations. Increased bandwidth requirements needed to handle modern communications technology are pushing up these costs. Law enforcement and national security agencies should be granted reduced line tariffs as provided in section 27 of the *Telecommunications Act*.

5. Law enforcement agencies recognize that CSPs should be able to recover reasonable costs incurred in providing court-ordered assistance, but are strongly opposed to those costs being paid for by police forces, most of which do not have the necessary resources.

6. Cost recovery by CSPs should be broadly and equitably distributed, as well as being reasonable and proportional to the actual assistance provided - like the 911 fee on phone bills. Charges should also be subject to independent third party review.

7. Any CSP charges authorized by the proposed legislation should be consistent and applied in accordance with a standard practice across Canada. The fees should be reviewed every two years with a specific date set for changes to be implemented.

8. After a date proclaimed by Cabinet, CSPs should be given a fixed period in which to provide information about the lawful access capabilities of their network. The information that a CSP provides about the upgrades or modifications necessary to meet legislated capabilities should be used to determine what assistance and reimbursement the CSP will receive to meet the requirements.

[18] The cost of new equipment or the updating of existing equipment.

## G. General Production Orders

1. Production orders of the type outlined in the consultation document make sense in today's world. Third party custodians of information can usually find it much more quickly and with less disruption to their other activities than law enforcement agencies. A production order could also help secure information in the control of, but not in the possession of, third parties - including information stored outside Canada.

2. The use of anticipatory investigatory techniques is very common in the successful resolution of criminal cases. The establishment of a production order empowering a judge[19] to authorize the monitoring of transactions over a specific time period is a logical and common sense proposal which is consistent with the law as it stands today[20]. It represents a reasonable compromise between the obligation to obtain a search warrant for information with higher confidentiality and free access to information without any form of judicial authorization.

3. Search warrants should only be required for information that tends to reveal intimate details of the lifestyle and personal choices of the individual affected by the order [21].

4. Production orders should be issued by a judge who is satisfied by a declaration under oath (or affirmation) by the investigating officer concerned that he/she is engaged in the bona fide execution of a lawful duty and that the order is reasonably required to allow this duty to be carried out.

## H. Specific Production Orders for Traffic Data

1. There are no *Criminal Code* provisions at present that address the collection of traffic data. A specific production order should be established for the acquisition of traffic data obtainable under a similar process to that for dialled number recorders (DNRs).

2. The definition of traffic data given as "telecommunications associated data" in the consultation document should be adopted in the proposed legislation.

3. Section 492.2 of the *Criminal Code* should be expanded to allow acquisition of DNR and traffic data where it is reasonably expected that the information may enable law enforcement agencies to prevent imminent bodily harm or death of any person - even if an investigation into a possible criminal offence is not involved.

## I. CNA/LSPID Information

1. Accurate and accessible subscriber information is an essential investigative and evidentiary tool. Authorities must have the ability to determine the owner of an account or service.

2. Customer name and address and local service provider information (CNA/LSPID) is not personal information and should not require judicial authorization to obtain it. However, CSPs are not compelled to produce this information on request at present. A statutory provision should be created requiring CSPs to provide law enforcement and national security agencies with CNA and LSPID information. If this is rejected on privacy grounds, a production order with a nominal procedural threshold should be considered instead.

---

[19] Where the word "judge" is used in this report, it should be taken to mean "judge or justice".

[20] *Criminal Code* s. 487.01 and s. 529(1) and *R v. Noseworthy* (1997) 33 O.R. (#d) 641 (Ont. C.A.) - cited by respondent.

[21] *R v. Plant* (1993) 3 S.C.R. 281 - cited by respondent.

3. CNA/LSPID information is critical to law enforcement's role in Canada and to meeting its international cooperation commitments. The maintenance of CNA/LSPID records should be made a prerequisite for CSPs conducting business in Canada. The fact that they operate in a competitive business environment should not relieve them of the fundamental responsibilities of Canadian corporate citizenship.

4. A national database could be set-up for CNA/LSPID information, populated by CSPs and accessible by law enforcement and national security agencies. It could be run and maintained by a private sector company selected through competitive bidding as in Australia or possibly a public/private partnership.

5. Alternatively, a distributed data system could be established allowing requests from law enforcement agencies to be automatically directed to individual CSP databases through an intermediary system. Results would be passed back to law enforcement via the same route. Whichever system may be chosen, security measures would be required to prevent unauthorized access.

6. The federal government should be responsible for funding the selected system.

**J. ASSISTANCE ORDERS**

1. Judges may already issue an assistance order under section 487.02 of the *Criminal Code*. However, this section should also be expanded to include reference to production orders.

**K. DATA PRESERVATION ORDERS**

1. Electronic forms of evidence are inherently volatile, so a mechanism is needed to ensure that evidence is not lost or destroyed before authorities can secure appropriate judicial authorization to seize it. The process for granting such an order should be streamlined and should reflect the fact that privacy interests are minimally affected when a third party, such as an ISP, is simply required to preserve data already in existence.

2. Where an authority is provided to order a service provider to preserve data temporarily, law enforcement agencies cannot subsequently seize that data without meeting the test of judicial authorization as would be required for any other search warrant.

3. The investigating officers, or designated law enforcement officials, should be authorized to issue exigent preservation orders valid for seven business days. Within this period, law enforcement agencies would be required to get judicial approval to extend the preservation order for up to 90 days.[22] CSPs should be notified of the date and time when the judicial preservation order will be served at the time of being served with an exigent order.

4. Preservation orders should apply to stored computer data as well as to paper records.

5. Preservation orders should be issued by a judge who is satisfied by a declaration under oath (or affirmation) by the investigating officer concerned that he/she is engaged in the bona fide execution of a lawful duty and that the order is reasonably required to allow this duty to be carried out.

[22] See statutory precedent in s. 487.11 and s. 529.3(1) of the *Criminal Code* - cited by respondent.

6. Legal standards need not vary depending on the type of data to be preserved. The nature of the data should only be considered when it is to be acquired by law enforcement agencies rather than simply preserved by a CSP or other custodian.

7. The time period for preservation of data should be a maximum of 90 days as stipulated by the *Convention on Cybercrime* - subject to subsequent extensions being granted by the courts for just cause.

8. The existing *Criminal Code* offences of "Obstruction of Justice" and "Disobeying an Order of the Court" as well as the common law offence of contempt of court are sufficient to deal with deliberate non-compliance with a preservation order.

### L. VIRUS DISSEMINATION

1. The infrastructure of the Internet should be given protection against malicious and damaging attacks by the addition to the *Criminal Code* of the offences of possessing, creating or selling a virus without lawful reason.

2. Canada's legislation should be uncompromising and in line with comparable laws in other western democracies and with the *Convention on Cybercrime*.

### M. INTERCEPTION OF E-MAIL

1. Canadian law enforcement welcomes the government's proposal to clarify the existing laws as they relate to the interception and seizure of e-mail.

2. The ways in which existing Canadian laws apply to the interception and seizure of e-mails are confusing and should be clarified. Access to e-mail content and its seizure should always be subject to prior judicial approval. However, seizure of this material does not appear to meet the definition or procedural requirements of interception. An e-mail is more like a letter sent through the postal system which should be seized under the search warrant provisions of the *Criminal Code*.

3. A specific *Criminal Code* provision should be created covering court-ordered acquisition of e-mail.

4. The stage of the transmission of an e-mail should be an irrelevant consideration in determining the type of the order required to acquire it. Moreover, the higher procedural safeguards that apply to the acquisition of voice communications should not be required in order to access e-mail data.

5. People talking on a conventional phone or a cellphone can reasonably conclude that no copy will be made of their conversation. This cannot be said of e-mail communications over the Internet. An e-mail consists of text that often passes through a number of third party computer systems where copies are made of the message before it reaches its destination. So the degree of privacy that could be reasonably expected when using e-mail would not be the same as that when using transitory verbal communications over wireline or wireless communications networks.

### N. OTHER TOPICS INTRODUCED BY RESPONDENTS

#### Video Intercepts

1. Section 487.01(4) of the *Criminal Code* has provided the police with an effective tool to fight serious crime. However, it requires video interceptions to be carried out exclusively by police officers. This is a serious drain on police resources today.

2. Trained civilian monitors, who are already involved in interceptions authorized under Part VI of the *Criminal Code,* can readily handle video intercepts as well.

3. Section 487.01(4) of the *Criminal Code* should be amended to allow video intercepts to be executed not only by a police officer, but by a person acting under the direction of a police officer.

**Target-Based Communications**

4. Part VI interception orders authorized by the courts specify the location at which the interception will take place. This approach presented no problem when most interceptions were on wireline services involving conventional phones, but it is not applicable to today's highly mobile wireless services such as two-way paging, wireless e-mail and coded numeric paging.

5. Some law enforcement agencies express the view that subsections 185(1)(e) and 186(4)(c) of the *Criminal Code* should be amended by replacing any references to the location of the interception with a description of the devices[23] to be intercepted.

6. Others propose that intercept orders be restructured to authorize the interception of the communications of a particular subject rather than specified pieces of equipment believed to be held by the subject. They point out that technology now allows an interception subject to add new devices and to discontinue use of previously held devices on a daily basis.

7. Any amendment that may be adopted should not apply to Part VI warrants authorizing entry to premises to install a listening device, where the requirement to describe the location of an interception would obviously still be necessary.

**Live Monitoring**

8. Law enforcement is seriously concerned about the rising costs of compliance with the live monitoring clauses included in most judicial authorizations under Part VI.

9. Live monitoring requires an authorized person to listen to a private communication being intercepted long enough to decide whether it can be lawfully intercepted or not. If it cannot be listened to in its entirety, the listener will "drop" the call.

10. Automatic monitoring records all the private communications associated with a given device for later review and analysis. The person who plays back the automatic recording is able to "block" any communication which is not authorized for interception in the same way as the live monitor. The call block protocol maintains a record for later inspection by a court of how much of a given interception was listened to by law enforcement agencies and how much has never been heard.

11. The *Criminal Code* should be amended to dispense with the live monitoring requirement, where call block facilities are available to an intercepting agency.

**Pre-paid or Pay-As-You-Go Services**

12. Pre-paid/pay-as-you-go cellphones, Internet access cards, Internet cafés and Internet facilities at public libraries all pose an obstacle to law enforcement agencies because the identity of the service user is easy to conceal from law enforcement.

[23] CACP submitted that a definition of the term "device" should be added to Part VI.

13. In keeping with the principle that no intercept safe havens be created, regulatory obligations should be established in Canada requiring the identification of users of prepaid communications services and the maintenance of an accurate subscriber database by the service provider.

**Cross Border Interceptions**

14. Several Canadian wireless companies and satellite communications system operators have service areas that overlap the Canadian/US border. This can mean that the subject of a Canadian authorization may be physically located in Detroit, although the interception itself is being carried out on a wireless switch located in Windsor.

15. The *Criminal Code* should be amended to make wireless and satellite cross border intercepts legally admissible as evidence in the courts, provided the interception takes place on a telecommunications facility in Canada.

16. When the service provider is in the US and the subject of a Canadian authorization is in Canada, the situation becomes more cumbersome. The only current means of gathering evidence in the US is by means of letters rogatory[24] which are subject to judicial approval or by invoking a mutual legal assistance treaty, if it exists. New expedited procedures or agreements should be put in place to provide rapid assistance. A central location in each country where this data could be retrieved would be very valuable to law enforcement agencies on both sides of the border.

**Communications Service Providers with No Infrastructure in Canada**

17. Canadians can obtain Internet services from a number of companies which, although they have an office in Canada, have their entire infrastructure located in the US. This means it is not possible to execute an interception authorization in Canada.

18. Legislation should be created that would compel all CSPs offering services to Canadians to have intercept capability available in Canada. Any new infrastructure costs incurred in order to comply with this requirement would be the sole responsibility of the CSP.

**Mobile Wireless Networks and Personal Digital Assistant Services**

19. The high-speed data overlay network[25] quite recently introduced by Personal Communications Service (PCS) providers presents lawful interception difficulties to law enforcement. This challenge will become tougher to tackle with the arrival of the very high-speed 3G mobile wireless networks.

20. Likewise, paging and Personal Digital Assistant (PDA) services can be hard to intercept without close cooperation from the manufacturers, because they use proprietary algorithms.

21. CSPs should be prohibited from using any technology that precludes lawful interception, regardless of whether they are the manufacturer or the purchaser of the technology.

[24] A letter rogatory is a request from a court in one nation to a court in another nation to enforce an order for deposition or discovery of evidence.
[25] General Packet Radio System or 2.5G network.

# CHAPTER 4: COMMENTS BY INDUSTRY

**Total Number of Written Submissions Received: 19**

The number of stars allocated to each item provides an indication of how frequently respondents expressed that opinion or one similar to it. Five stars denotes "very frequently". One star generally indicates a single response on the topic, although it may have been made on behalf of an industry association or group representing a number of organizations. The listing of a given group (or groups) of respondents beside each comment indicates that at least one participant from that group expressed that view or one much like it. Respondents in this section are listed in Annex B.

The abbreviation **CSPs** is used in this chapter to denote comments by one or more of the following communications service providers or their industry associations:
**Telcos** - Major national or regional carriers such as incumbent telephone companies, inter-exchange carriers and competitive local exchange carriers (CLECs)
**Internet Service Providers** (ISPs)
**Wireless Service Providers** (WSPs)
**Fixed Satellite Services** (FSS)

## A. GENERAL

1. The consultation document lacks detail and is too imprecise to allow anything but high-level comments. It does not form the basis for meaningful consultation. CSPs, Banks[26] *****

2. Further consultation is called for, including the opportunity to comment on the specific proposals contained in draft legislation and accompanying regulations, prior to introduction in Parliament. CSPs, Banks *****

3. Most service providers who responded[27] support lawful access and the ability of Canadian law enforcement and national security agencies to undertake lawful interception of communications in the face of technological change, subject to the protections afforded Canadians under the *Canadian Charter of Rights and Freedoms*. CSPs ****

4. The interception of unviewed e-mail and similar digital communications traffic in transit should be considered interception of a "private communication" and therefore subject to the protections contained in a *Criminal Code* Part VI authorization. A search warrant or production order should be required for law enforcement to access opened e-mail that a user has chosen to retain. CSPs, IT[28] ****

5. The consultation document failed to show that the current provisions in law are inadequate to allow effective access to data communications services in Canada or that investigations/prosecutions have been unsuccessful due to lack of technical capability. CSPs, IT ***

[26] Denotes comments by respondents from the banking industry.
[27] The others did not express a view on the matter.
[28] Information technology industry/associations. Note: Unlike other industry respondents, the IT category includes manufacturers of telecommunications-related hardware and software.

6. The proposed legislation should impartially balance the maintenance of lawful access capabilities with the need to provide new and innovative telecommunications services in Canada while enhancing the efficiency and competitiveness of the Canadian market. CSPs ***

7. Industry must be fully involved in the design and implementation of the technical standards and requirements which may be mandated by regulation. A government/industry working group may be the best way to handle this task. CSPs **

8. There appears to be no public benefit in proceeding with haste to implement this legislation at the expense of adequate consultation. Technical standards and equipment solutions are unlikely to be available for a number of years and law enforcement representatives have expressed general satisfaction with the positive working relationships they have developed with major carriers and ISPs to date. CSPs **

9. The Council of Europe's *Convention on Cybercrime* has not been ratified by Parliament in Canada - in fact only two countries that signed the *Convention* in Budapest in 2001 have ratified it so far. This makes it a weak basis on which to justify increased lawful access. CSPs**

10. WSPs are opposed to any obligation that may cause the elimination of certain services or classes of services, such as pre-paid wireless. CSPs **

11. The consultation document fails to offer balancing measures to protect the public interest and to prevent the misuse of the proposed powers. CSPs **

12. Wireless service providers are currently operating under the *Solicitor General's Enforcement Standards* which refer to *CALEA*[29]-style wireline telephony interception. WSPs take strong issue with the idea that these same standards should apply to services offered using packet-based switching. The industry is looking for clarification on what will happen to their existing conditions of licence and these standards when the new legislation comes into force. CSPs *

13. The government's position on data retention and treatment of user encrypted data communications is not stated in the consultation document. These issues are too important to be overlooked. IT *

**B. REQUIREMENTS TO ENSURE INTERCEPT CAPABILITY**

1. The term "telecommunications facility" is not defined in the consultation document (although it appears several times in the text). Definitions provided in the consultation document differ from those given in the *Telecommunications Act*. Clear consistent definitions in line with those used internationally are essential to the success of the proposed legislation. CSPs ***

2. The addition of a single piece of new equipment with increased interception capabilities into a network should not trigger a requirement for the service provider to upgrade the whole network in question. CSPs ***

3. The manufacturers of some software-enabled lawful access capabilities require both the installation of the software package concerned and the purchase of a "right to use" (RTU) licence - which can be costly - before certain features can be turned up. Service providers suggest that the proposed legislation require them to maintain the general software capability and to activate

[29] *Communications Assistance for Law Enforcement Act* - passed into law by the US Congress in 1994.

particular features involving RTU licences only when a request is received from law enforcement agencies requiring that feature. CSPs ***

4. Canadian banks wish to be assured that their operation of extensive communications networks and related facilities does not qualify them as *service providers* under the proposed legislation. The same question also arises for a number of private corporations, hotels, universities and government departments. Banks, IT ***

5. Some CSPs stress that when smaller operators (like Internet cafés) offer competing services to the public, they should be designated as *service providers* under the proposed legislation., CSPs ***

6. Service providers should not be obliged to develop lawful access solutions for services or technologies where no solutions are yet available from vendors, since costs could very well be prohibitive. CSPs ***

7. Service providers should not have to provide lawful access to network systems that they use for provision of services, but which are owned and controlled by others. CSPs ***

8. All service providers competing in the same market should be subject to similar lawful access requirements whether they are facilities-based, re-sellers or third-party providers. At the same time, regulations or standards must be flexible enough to accommodate the different technologies used by the carriers involved. CSPs **

9. Larger service providers should not be responsible for infrastructure or operational assistance for lawful access to private line or wholesale services, which should be the legal and financial responsibility of the end-user service providers. CSPs **

10. Satellite communications service providers are poorly placed to provide useful lawful access and have no wish to incur the costs involved. They act as carriers for other carriers involved in telephony and Internet services. Commonly they own no ground facilities involved in these networks. In their view, surveillance is best carried out at end-user service providers (like ISPs) and ground-based carrier facilities - as has been the case traditionally. CSPs *

11. Where service providers use encryption within their networks, they should be allowed to choose either to provide a key or to deliver unencrypted text when required to do so by law enforcement agencies. IT *

12. "Significant upgrade" should be defined as the replacement of, or substantial modification to, the entire hardware and software platform used by the service provider's core network. CSPs *

13. "Core network" should mean the physical entities that provide support for the network features and telecommunications services - including those that deliver subscriber location information, network control, switching and transmission. CSPs *

**C. REGULATIONS**

1. Most CSPs agree that it is crucial to know and understand what is required of them by law enforcement. CSPs ****

2. Service providers are opposed to the imposition of uniquely Canadian requirements for lawful access. It is most unlikely that telecommunications equipment manufacturers will develop Internet or

wireless intercept-ready solutions especially for the Canadian market. If they do, the solutions will almost certainly be expensive and proprietary. CSPs ****

3. What do "general operational requirements" and "basic intercept capability" mean? Will the existing capabilities being offered to law enforcement agencies meet the standard? What about interface specifications? CSPs ***

4. Technical standards for lawful access should be prepared by industry experts and agreed by industry-government working groups. As long as the required intercept functionality is provided, the network design to achieve this should be up to the service provider. CSPs, IT ***

5. Ultimately, the responsibility for developing compliant equipment should rest with the manufacturers. Any off-the-shelf solutions meeting US legislative requirements should be accepted as compliant in Canada. CSPs, IT ***

6. Some companies have incurred significant personnel and overhead costs in responding to lawful access requests which they have experienced difficulty in recovering. The regulations, or the legislation itself, should make it clear that reasonable compensation is payable for operational assistance (see F2 below). CSPs **

7. Apart from specifying the need for appropriate security clearances, the regulations should not set standards for the competence, reliability and deployment of service provider employees. This should be the responsibility of the employer. CSPs **

8. Lawful access capabilities should be required in all new voice or data services equipment being considered for the Canadian telecommunications market. CSPs *

9. Regulation is a method of implementing law that does not undergo the same level of public scrutiny as a statute. IT *

10. Issues such as distribution of costs, technical and operational standards and duties of a service provider in response to an interception order are far too crucial to the industry to be relegated to regulations instead of the full parliamentary review they deserve. CSPs *

**D. FORBEARANCE**

1. Clear and consistent forbearance criteria should be established. The process dealing with all forbearance requests should be fair and transparent. CSPs ***

2. Forbearance may create identifiable safe havens for criminals. CSPs ***

3. Some WSPs said that any service provider that is unable to meet the basic minimum intercept requirements should be obliged to seek forbearance. Other WSPs maintained that service providers should be allowed to request forbearance from any requirements that they cannot reasonably be expected to satisfy. CSPs **

4. The industry should be involved in the drafting of administrative guidelines to govern the management of forbearance requests. CSPs **

5. Although forbearance may be needed for the evaluation of experimental services for limited periods, it is not clear that a general forbearance policy is necessary. Interception solutions are available for almost all public telecommunications services currently in use. IT *

6. Any forbearance regime should not competitively disadvantage compliant service providers compared with non-compliant ones. CSPs *

**E. COMPLIANCE MECHANISM**

1. ISPs must be provided with clear guidelines and procedures to follow when they are served with a court order. CSPs **

2. Larger service providers suggest that their compliance should be determined based on the results of their regular cooperation with law enforcement and security agencies and that smaller providers be subject to law enforcement-funded inspections carried out by the Solicitor General. Having each law enforcement or national security agency conduct its own inspections would likely be unworkable. CSPs **

3. Some service providers strongly oppose a system involving regular or random inspections to determine compliance or one that calls for service providers to register their compliance, on the grounds of cost. It would also mean more bureaucracy. CSPs **

4. Contempt of court is an adequate deterrent for failure to comply with warrants, production orders, etc. Summary conviction offences may be needed to deal with consistent and unjustified non-compliance with lawful access capability requirements. CSPs **

5. Sanctions should only be imposed if a service provider is unable or unwilling to meet its obligations when served with a properly authorized judicial order. CSPs *

6. Any new compliance regime should be based on the successful model used to track lawful access compliance by Personal Communications Service (PCS) licensees in Canada since 1996. CSPs *

**F. COSTS**

1. Service providers should not have to pay for providing basic intercept capability regardless of how "significant upgrade" and "new service or technology" are defined in the resulting legislation. Until technical solutions are readily available for the transmission equipment used by service providers, that can be deployed and maintained at minimal incremental cost to the service provider, the government should pay for the "basic intercept capability" (however characterized). CSPs, IT *****

2. The legislation should ensure that law enforcement agencies remain responsible for reasonable costs incurred by service providers making available operational assistance to law enforcement agencies in carrying out lawful interception, seizure and preservation orders. These costs should be worked out between each service provider and the agency concerned rather than being based on universal tariffs laid out in the regulations for various types of support. Industry Canada and the Solicitor General, or an independent arbitrator, should mediate any disputes about fees for service between a service provider and a law enforcement agency. CSPs, IT *****

3. Providing lawful access for law enforcement agencies generates significant on-going costs in terms of personnel, training and security requirements, in addition to the specific costs of implementing an interception capability. CSPs ****

4. The costs of making upgrades and keeping new technologies accessible to law enforcement agencies in Canada amount to a government tax on technical innovation by ISPs. If they are not reimbursed by the government, these costs will have to be passed on to consumers, reducing

competitiveness and creating a strong disincentive for technological innovation and investment by Canadian ISPs. CSPs, IT ***

5. Care must be taken to ensure that lawful access capability requirements do not create a windfall for telecommunications equipment manufacturers. It is inequitable that service providers are held to cost recovery when providing assistance to law enforcement agencies, while equipment manufacturers are subject to no pricing restraints when selling service providers the equipment and software necessary to provide lawful access capability. CSPs ***

6. Lawful access is carried out in the public interest and should be paid for by Canadian taxpayers at large. CSPs ***

7. In the absence of any argument that CSPs are faced with an unjustified financial burden, the cost of providing lawful access should be borne by industry as a civic duty. IT *

8. The high cost to small service providers of compliance with the proposed interception capabilities and their maintenance could cause these companies serious and irreparable financial harm. CSPs *

9. In the undesirable event that service providers are ultimately compelled by the proposed legislation to cover the costs of lawful access, the legislation should provide that all service providers, including those whose rates are regulated, will be able to recover these additional costs from their customers. CSPs *

### G. General Production Orders

1. Service providers should be allowed a reasonable time to respond to a production order depending on the nature of the data, the number of sources to be searched and the facilities available to carry out those searches. CSPs **

2. The definition of "telecommunications associated data" given in the consultation document should be amended by adding the following phrase to its last sentence - "that does not reveal, directly or indirectly, material details of the content of the transmission". CSPs *

3. Legal instruments authorizing access should be an order of a superior court - approval by a justice of the peace is not a sufficient safeguard. IT *

4. Service providers oppose "anticipatory orders" as they appear to oblige a custodian to produce documents that are not yet in its possession and that may be unlikely to come into its possession in the normal course of business. CSPs *

5. Any new legislation should include provisions to protect service providers from criminal and civil liability when complying with the terms of a judicial order. Section 25 of the *Criminal Code* does not provide adequate protection in all cases. CSPs *

6. The consultation document refers to searches against third party custodians, like banks and companies, where the bank or company does the searching on behalf of law enforcement agencies within an agreed period of time. ISPs want to know how this type of production order might apply to them. They say it is not clear when an IP packet might become a document or at what stage in communicating an e-mail message the ISP might become a custodian. CSPs *

7. The use of the term "document" in a data network context can be confusing and should be clarified. E-mails and e-mail attachments are pretty clearly documents, but what about web pages, instant messages, peer-to-peer traffic, instant relay chat messages and log files? IT *

8. The consultation document suggests that production orders will facilitate seizure of documents stored in a foreign country. It does not examine, however, what happens if the foreign country rejects the order or whether Canada will recognize incoming foreign production orders. IT *

9. If investigatory data is likely to be shared extra-territorially, the legal instrument authorizing the surveillance should be approved by a superior court judge. IT *

### H. Specific Production Orders for Traffic Data

1. Internet "telecommunications associated data" can be more privacy invasive than the equivalent telephony data. For example, Internet search engine records can over time reveal intimate personal information. Interception of this type of information should be subject to judicial oversight. Moreover, the definition of "traffic data" should be narrowly constructed - as it appears to be in the *Convention on Cybercrime*.[30] CSPs, IT ****

2. All the procedural safeguards currently applicable to intercept orders should be maintained where there is any possibility that the data relates to or provides access to the content of a communication or could be used or manipulated to determine or suggest the content of a communication. CSPs ***

3. Preservation and production orders should apply only to data that is clearly under the control of telecommunications service providers and not to user-managed data, even if resident on the service provider's facilities. CSPs **

4. Some ISPs support the use of a lower standard for the production of telecommunications associated data and CNA information, as is the case in telephony lawful access. CSPs *

### I. CNA/LSPID Information

1. There is strong opposition against obliging service providers to collect, maintain or guarantee the accuracy of subscriber information beyond that needed for their own business purposes. The *Personal Information Protection and Electronic Documents Act (PIPEDA)* limits the collection of unnecessary personal data and its retention for periods beyond normal business requirements. Communications service providers are not an arm of law enforcement and should not be transformed into one by this proposed law. CSPs, IT *****

2. Service providers are also strongly opposed to the creation of any national subscriber database citing privacy and security concerns, as well as the high costs of developing and maintaining database accuracy. They point out that most cybercriminals are quite capable of using false names, hacked accounts or public access terminals to communicate or transact. CSPs ****

3. If it is determined that a service provider customer name and address (CNA) database is required, its operation for law enforcement purposes should be coordinated by a third party independent of both law enforcement and service providers. Each service provider database should contain the name and address data associated with wireline telephone service only. CSPs *

---

[30] "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration or type of underlying service." Chapter 1, Article 1(d) - cited by respondent.

**J. ASSISTANCE ORDERS**

1. Service providers are highly supportive of assistance orders which spell out clearly and specifically what is required of the service provider. CSPs ***

2. Some larger service providers say they know their networks far better than law enforcement agencies ever will and are therefore keen to offer assistance in the execution of warrants/orders, without the need for legal compulsion. CSPs **

**K. DATA PRESERVATION ORDERS**

1. Strong opposition was expressed to any data retention obligation due to cost and staffing impacts, as well as substantial technical demands on networks. Reasonable limits should be applied to the amount of data to be captured, stored and delivered under a preservation order. CSPs ***

2. Larger service providers are generally supportive of the introduction of preservation orders into Canadian law as long as they are explicit and unambiguous, narrowly targeted, short in duration and they allow service providers a reasonable time to comply. CSPs **

3. The concept of "exigent circumstances" preservation orders without judicial authorization is also acceptable to larger providers, provided the data is only to be preserved for the time taken to obtain a court order, which should not exceed four days. A fully documented "exigent request" should be provided together with explicit limitation of liability for the service provider. CSPs **

4. The preservation period should not exceed 90 days - as required in the *Convention*. If prospective isolation, filtering or interception of data is required by law enforcement agencies rather than simple storage of raw data for a limited period, the order should be subject to the highest standard of judicial authorization. CSPs **

5. A G8 report[31] says that data preservation does not compel either collection or retention of data - it is essentially a "do not delete" order covering existing data. This assumes that a given ISP is already collecting the data concerned, otherwise there will be no data to preserve. In practice, there is often little business requirement for ISPs to collect or retain traffic data. CSPs, IT **

6. A data preservation order contemplates the issuing of a further order such as a production order or a search warrant at a later time. Law enforcement agencies should be required to demonstrate that they are likely to obtain that subsequent order or warrant successfully, before the preservation order is authorized. Banks *

7. It should be made clear in the legislation that data preserved under a preservation order will only be accessible by the authorized agency for law enforcement or national security purposes. It will not be available to those agencies or other persons or organizations for any other purpose or legal process, such as a civil subpoena. CSPs *

8. Data preservation orders should carry the same judicial standard as a search warrant to ensure that orders are not used trivially by law enforcement agencies. CSPs *

[31] *Data Preservation Checklists*, available at http://www.g8j-i.ca/english/doc4.

## L. VIRUS DISSEMINATION

1. The legislation should require law enforcement agencies to show that criminal intent existed for an offence to have occurred. This is important for software labs, service providers, common carriers and security specialists whose work demands that they possess viruses for legitimate testing purposes. CSPs, IT ***

2. The legislation should make it clear that service providers will be exempted from any liability if they have no actual knowledge of the existence of the viruses on their networks. CSPs, IT ***

## M. INTERCEPTION OF E-MAIL

1. The key to appropriate lawful access to e-mails[32] lies in whether the message has been received (read or viewed) by the intended recipient. If the message has not been received (keyboarded, unsent, not arrived, unopened, etc.) it should be regarded as a "private communication" in transit and subject to lawful access in the same way as wiretaps under section 186 of the *Criminal Code*. ISPs, Telcos, IT, ****

2. The legislation must make it clear at what stage in the transmission of an e-mail interception or seizure is to take place and how it should be undertaken. ISPs **

3. Users of chat, SMS[33] messages and similar services have a reasonable expectation of privacy given the transient nature of the communications. The "private communication" definition should be broadened to explicitly capture these other services as well as e-mails. CSPs **

4. There is less expectation of privacy when it comes to stored material, since it can be viewed and distributed to others. A search warrant or production order should be required for lawful access to stored communications. CSPs **

5. Not all e-mail systems distinguish between "opened" and "unopened" e-mails. So on some systems, for example, it may not be possible to execute warrants requiring seizure of "opened" emails. CSPs *

## N. AMENDMENTS TO THE COMPETITION ACT

1. There seems to be general support for judicially-authorized access by the Competition Commissioner to hidden records, as well as recourse to assistance and production orders under *Criminal Code* safeguards. CSPs **

## O. OTHER TOPICS INTRODUCED BY RESPONDENTS

1. Some respondents pointed out the challenges involved in balancing the public's basic right to privacy against law enforcement's need to access data that will allow it to carry out criminal investigations effectively and to assure the security of the state. A number of respondents expressed the view that the proposed legislation could well tip that balance in favour of excessive intrusion by law enforcement agencies to an extent that could be difficult to reverse. CSPs **

[32] And similar text-based telecommunications.
[33] Short Message Service.

# CHAPTER 5: COMMENTS BY CANADA'S PRIVACY AND INFORMATION COMMISSIONERS

**Total Number of Written Submissions Received: 5**

**A. GENERAL**

1. Interception and monitoring of private communications is highly intrusive - striking at the heart of the right to privacy. The burden of proof must always be upon those who claim that some new intrusion or limitation on privacy is necessary.

2. Any such proposed measure must meet a four-part test:

- It must be demonstrably necessary in order to meet some specific need.
- It must be demonstrably likely to be effective in achieving its intended purpose.
- The intrusion on privacy must be proportional to the security benefit derived.
- It must be demonstrable that no other, less privacy-intrusive, measure would suffice to achieve the same purpose.

3. The proposed measures risk stirring up public distrust in information technology and communications generally, in the belief that they are intercepted all the time or at least that they are susceptible to interception.

4. The proposed powers of access to the private communications of Canadians go far beyond maintaining the capabilities and authorities available to law enforcement and national security agencies in the past.

5. If extended powers are indeed believed to be necessary, they must only be used and deployed to meet legitimate law enforcement objectives. The information collected through these powers must not be used for purposes unrelated to public safety.

6. There is also a responsibility on the part of law enforcement officials to protect the confidentiality of that information, particularly if it proves to have no relevance to their investigations.

7. The three departments involved in the proposal should present a clear statement of the problems faced, together with operational evidence supporting the need for enhanced interception and surveillance powers proposed in the consultation document.

8. Concern for the protection of privacy from unnecessary erosion should extend beyond the proposals outlined in the consultation document. In the past year, Canadians have been faced with legislation unprecedented in its capacity to diminish the privacy of individuals. This included the *Anti-terrorism Act*, Omnibus Bill 42[34] and the privacy-invasive provisions of the Canada Customs and Revenue Agency's air traveller surveillance database. The introduction of this legislation was fragmented, with no clearly articulated context and with limited consultation or discussion.

9. Privacy is a constitutionally protected right. Privacy in electronic communications should only give way to law enforcement and national security needs where those needs clearly outweigh the privacy interest and then only to the minimal extent necessary. The existing *Criminal Code* provisions dealing

[34] Later Bill 42 became Bills 44 and 55 (now C-17) - cited by respondent.

with interception of private communications appropriately balance individual privacy interests against the public interest in effective law enforcement.

10. The Government of Canada should only proceed further with the lawful access proposals if clear evidence is offered to support the need for changes. Most certainly, the Government of Canada should not proceed simply because it is expedient to do so in the post-September 11 climate of fear and insecurity.

11. It is worth noting that Australia, South Africa and the UK have recently experienced strong opposition to the enactment and implementation of new lawful access legislation with similar objectives to those outlined in the Canadian consultation document.

12. In spite of strict regulations on its use and the criminalizing of unauthorized access to the system, the government will be unable to prevent abuse of the system in practice.

13. Criminals will quickly detect that they are under surveillance and will use other means of communication, while most citizens will be targets of this vast system, unable to unplug all their telephones and other communications equipment.

14. No evidence has been offered that existing interception and search and seizure laws are inadequate for dealing with today's electronic communications, nor does the Council of Europe *Convention on Cybercrime* offer a persuasive rationale for the proposals. The proposals would weaken existing legal protections of privacy in Canada without a clear and compelling justification.

15. Canadians are entitled to feel confident that their communications and on-line activities will not be arbitrarily intercepted or scrutinized.

16. The *Convention* has not yet been ratified by Canada, so whatever legal obligation is being asserted to implement its provisions is in fact non-existent.

17. If the *Convention* calls for unjustifiable intrusion on the privacy rights of Canadians which is inconsistent with our values and rights, the *Convention* should not be ratified by the Canadian government.

18. The government has not shown in the consultation document how it will comply with Article 15 - Conditions and Safeguards - of the *Convention*, in particular how it will provide adequate protection of human rights and freedoms and how it will observe the principle of proportionality. One might also ask how the imposition of the *Convention* could comply with its own Article 15.

**B. REQUIREMENTS TO ENSURE INTERCEPT CAPABILITY**

1. Any new legislation dealing with interception and seizure of Internet communications content and traffic data should be as narrow and specific as possible. Routine and exploratory electronic surveillance on a large scale must not be allowed. Overbroad measures would impair privacy rights and run afoul of section 1 of the *Canadian Charter of Rights and Freedoms*.

2. New technologies and communications services may well pose a challenge to existing interception methods and require CSPs to provide law enforcement agencies with basic interception and surveillance capabilities to achieve lawful access to them.

3. As stated in the consultation document, these capabilities should maintain the status quo, allowing existing state powers to be effectively applied to the new communications services. That is to say, law enforcement and national security agencies should have the same ability to intercept and monitor e-mail and cellphone communications, for example, as is now the case with letter mail and conventional wireline telephone communications.

4. More information should be provided on how the intercepts would be carried out, by whom and for what purposes, together with proposals on evidentiary thresholds, oversight controls and safeguards before a reasonable assessment is possible on this issue.

5. Requiring service providers to acquire technical capacity to provide lawful access co-opts the private sector inappropriately in state surveillance. The costs to CSPs will raise consumer prices and may diminish the competitiveness of Canada's Internet providers. The development and implementation of Internet technology will be driven by the interests of surveillance rather than by the needs or realities of Canadian business and its consumers.

6. Carrying out interceptions on a traditional wireline telephone system is not comparable with monitoring wireless communications systems or the Internet which can provide more personal information and be more privacy invasive. A new approach is needed rather than simply extending existing procedures to address new technologies.

7. The infrastructure, tools and databases necessary to provide the proposed lawful access will attract substantial interest on the part of numerous criminal organizations, terrorists and the intelligence services of countries that are not signatories to the *Convention* and who will be unconcerned by any possible penalties imposed for breaking the rules on access to the system.

### C. DATA RETENTION AND PRESERVATION ORDERS

1. The government should continue to resist any suggestions that general *retention* requirements be part of the lawful access initiative.

2. Preservation orders are just as dangerous and inappropriate from a privacy viewpoint as retention orders. The concept of a preservation order does not exist in Canadian law, so the assertion that this type of authority is necessary to "maintain" existing lawful access capability cannot be so.

3. It is not clear from the consultation document what level of proof of suspected wrongdoing would have to be presented to a judge in order to serve a preservation order on a CSP. In some circumstances it appears that no proof would be necessary - the order would simply be issued by law enforcement or national security agencies.

4. The judge asked to approve a preservation order may be less inclined to insist on rigorous proof that it is necessary, since the information will not be handed over to law enforcement agencies at that time. Similarly, the second judge asked to order the actual production of the information may assume that the appropriateness of the whole intrusion has already been established before the first judge.

5. It is possible that preservation orders could be served that covered message content rather than traffic data. ISP preserved content could then be accessed subsequently by law enforcement agencies with a search warrant which is considerably easier to obtain than an interception order.

6. An order requiring preservation of information at an ISP introduces additional privacy risks such as data security at the ISP as well as potential unlawful access by hackers and others.

7. Provisions should not be drafted that would require ISPs to retain all traffic data and content for a specific period solely for the purposes of a hypothetical law enforcement action. Such measures would be overbroad and could seriously harm Canadian privacy, as well as the business of Canadian-based ISPs. Canadians could flee to ISPs based outside Canada to preserve their privacy and cause serious damage to an industry that underpins domestic electronic commerce.

8. The principle of data preservation orders presents no problem, but the breadth of Articles 16 and 17 of the *Convention*[35] certainly does and the proposed 90, 120 or 180 day periods are too long.

9. Preservation orders should only apply to stored computer data (not paper records). They should only be available to support an ongoing investigation into a possible violation of criminal law.

10. Law enforcement agencies, consistent with section 487.11 of the *Criminal Code*, should only be able to secure an exigent preservation order when it would be impracticable to obtain a judicial order in the circumstances.

11. Requiring ISPs to track all online activities of their subscribers, so that this information could potentially be used as evidence, would require a massive investment in storage capacity for the ISPs. This could cause them to increase their fees substantially, impeding the growth of online services in Canada. It could also result in industry consolidation with negative implications for privacy and free speech.

12. This massive aggregation of data will be of little use to law enforcement agencies unless they have adequate resources to review and analyze the vast amounts of data that would be collected daily.

### D. General Production Orders

1. The consultation document does not make the case for production orders - the need has not been established. However, a general production order has been proposed, which is like a search warrant without the need for a law enforcement officer to be present.

2. General production orders should be available only from a judicial authority applying existing standards. It seems unclear, however, why authority to compel CSPs to provide this information should be necessary now, when law enforcement agencies have traditionally been able to obtain it.

### E. Specific Production Orders for Traffic data

1. The assumption in the consultation document that traffic data necessarily involves a lower expectation of privacy should be called into question. In the case of regular telephone communication, telecommunications associated data consists merely of phone numbers dialled by a subscriber and the incoming phone numbers of callers who have attempted to contact that subscriber. By contrast, collection of telecommunications associated data related to e-mail and Internet communications can yield a great deal of information about the intimate details of Canadians' personal lives.

### F. CNA/LSPID Information

1. The consultation document suggests the creation of a national database containing customer name and address and local service provider information (CNA/LSPID) for all Canadian subscribers,

[35] Article 16 - Expedited preservation of stored computer data
Article 17 - Expedited preservation and partial disclosure of traffic data

because law enforcement/national security agencies are experiencing difficulty in identifying the local service provider associated with a given telephone number or subscriber. A national database of this kind should not be created.

2. If it involves some effort on the part of law enforcement agencies to obtain CNA/LSPID information, they will think twice before seeking to secure it. Moreover, a unique identifier like a phone number when associated with a person's name and address is worthy of privacy protection. There is no need to change the current law and practice concerning access to this information.

3. A centralized national database registry of Internet subscribers would allow law enforcement agencies to routinely trace an IP address back to the registered user rather than requesting this information from an ISP. If carried out, this proposal would obliterate any expectation of privacy and anonymity on the Internet.

4. Many people have multiple e-mail accounts, both at home and at work. It is also not uncommon for people to close accounts with one ISP and create new ones with another provider offering a better deal. The logistics of creating and maintaining a comprehensive national database of up-to-date e-mail customer account information looks unworkable and also represents a drain on resources better used elsewhere.

5. In addition to the belief that the creation of this database would further conscript the private sector into surveillance must be added concern about the proliferation of government databases containing information about Canadians.

6. This proposal should not be adopted. There has been no clear justification of need on the basis that the present means of collecting subscriber information are inadequate, or that such a database will actually work and not be circumvented by criminals.

7. The consultation document also suggests that all service providers be obliged by law to collect, verify and maintain a record of the identity and address of all their subscribers. This would include an obligation on those selling pre-paid cellphones or phone cards to collect (and communicate to ISPs) people's sensitive information, such as driver's license and credit card numbers, before making the sale. This would be a gross invasion of privacy.

### G. E-MAIL INTERCEPTION

1. These questions should have been put to Canadians directly during the consultation process:

- Should it be lawful to open an e-mail account in Canada without the client providing basic personal information for each e-mail address?
- What are the appropriate kinds of personal information that could be collected by Canadian ISPs?
- What degree of on-line anonymity would be permissible under the proposed amendments?
- Would anonymous re-mailing of e-mail within Canada remain lawful?
- Would encrypted e-mail be permitted within Canadian borders and, if so, on what terms?

2. An e-mail, which can contain text, sound and graphics files, is a rich source of intimate personal information about the sender and, potentially, about the recipient. The Alberta courts have affirmed that the recipient of the content of an e-mail enjoys a *Charter*-based reasonable expectation of

privacy in that communication.[36] Existing standards respecting interception of private communications should apply to e-mail interception. The issue of how much lower the expectation of privacy is in the case of an e-mail header was left unanswered by *R v. Weir*.

### H. OTHER TOPICS INTRODUCED BY RESPONDENTS

1. Nowhere does the consultation document indicate that accountability measures are being contemplated.

2. The proposals in the consultation document call for high levels of trust by Canadians in our law enforcement and intelligence communities, without offering corresponding evidence that this kind of legal change is needed.

3. Broad judicial and other oversight mechanisms should be built into the lawful access proposal to ensure public accountability, transparency and scrutiny.

4. An oversight body should be established to enhance public confidence. This organization should require routine reporting of lawful access measures undertaken by law enforcement as well as providing an assessment of the efficiency of these measures.

5. Independent oversight of the nature and frequency of use of any new lawful access powers is essential, subject to the proper protection of law enforcement interests. A body such as the Security and Intelligence Review Committee of Parliament should be considered for oversight of any new lawful access to e-mail and other electronic communications data.

[36] *R v. Weir*, [2001] A.J 869 (Ab.C.A.) - cited by respondent.

# CHAPTER 6: COMMENTS BY CIVIL SOCIETY GROUPS

**TOTAL NUMBER OF WRITTEN SUBMISSIONS RECEIVED: 14**

The number of stars allocated to each item provides an indication of how frequently respondents expressed that opinion or one similar to it. Five stars denotes "very frequently". One star generally indicates a single response on the topic, although that response may have been made on behalf of an association or group representing a number of organizations or individuals. Respondents in this section are listed in Annex D.

## A. GENERAL

1. The consultation document is unclear about what the Government of Canada is actually proposing. This means that comments by civil society groups must unavoidably be similarly vague. Participants look forward to responding to whatever legislative proposals are brought before a parliamentary committee. *****

2. The document is also unconvincing on how the legislative proposals would actually help fight organized crime or terrorism. Agencies of the state are likely to have much more access to the private lives of Canadians, but serious criminals and terrorists are unlikely to be careless enough to fall within the scope of the proposed measures. *****

3. The lack of clarity about evidentiary thresholds, oversight and safeguards makes it impossible to provide an opinion on this proposal. ****

4. The government's proposals for greater lawful access to private communications have not been demonstrably justified, according to the tests articulated by both the Supreme Court[37] and the Privacy Commissioner of Canada[38]. ****

5. If evidence is available to justify the proposed measures, it should be made public, so that Canadians can weigh it and thus make informed judgments as to whether the security benefits of the measures outweigh the privacy costs. If such evidence does not exist, the measures should be dropped. *****

6. Cybercrime, whether or not the problem is real, impending, or imagined is being used as a justification for proposed legislation that is in grave danger of curtailing rights of individuals to privacy. Canada should not ratify the *Convention on Cybercrime* if to do so would be inconsistent with Canadian values and rights set out in the *Canadian Charter of Rights and Freedoms* and interpreted by the Supreme Court of Canada. ****

7. The proposals would effectively establish a lower standard for lawful interception and/or search and seizure in the online context versus the offline context (telephone and postal mail, for example), yet no justification has been provided for this. *Criminal Code* standards should be designed to apply, regardless of technology.****

8. The draft legislation and accompanying regulations should be made available for full and complete public review with sufficient time for interested parties to assess their impact and submit their comments. ***

[37] *R v. Oakes* [1986] 1 S.C.R. 103 - cited by respondent.
[38] Comments on *Lawful Access Consultation Document*, November 25, 2002 - cited by respondent.

9. The consultation document states that the objective of the lawful access proposals is "to maintain lawful access capabilities for law enforcement and national security agencies in the face of new technologies". Instead, the proposals would significantly *increase* the ability of the agencies to intercept, search and seize electronic communications of individuals and personal information about individuals in electronic form. ***

10. The purpose of a consultation process is to gain useful feedback from stakeholders and to use that feedback to shape better legislation. The success of such a process requires full and frank disclosure of what the government intends to do. The lawful access consultation process appears not to have proceeded in this manner. ***

11. The proposal that law enforcement and national security agencies need to "maintain lawful access capabilities" in the face of technological developments should be rejected. Not only would the proposal increase such capabilities beyond their present scope, but section 1 of the *Charter* requires that restriction of rights must be "demonstrably justified" and that they be consistent with "a free and democratic society". No such need has been empirically demonstrated.***

12. Civil society groups would like to see statistics justifying the need for the proposed changes. The case for new powers has not been well-documented. ***

13. The broad working definition of "service provider" to include universities, colleges and libraries that provide Internet services to the public is a matter of concern.***

14. The Internet may be relatively new, but the fundamental values of privacy and civil liberties have not changed. Our rights were won and preserved by the sacrifice of earlier generations, often in the face of threats far greater than anything that exists today. Respect for them, and for the country they have left us, makes it unthinkable that we should surrender these rights now, whether on the pretext of fighting terrorism, or of imitating a bad European or American law. ***

16. The lawful access related obligations under the *Convention* go further than the proposals in the consultation document. They include disclosure of crypto keys and new criminal offences relating to child pornography and real-time monitoring of data communications. All such obligations should be the subject of consultation before the *Convention* becomes law in Canada. **

17. Our sense of what it is to live in a democracy requires that the state should not interfere with, or restrict the rights, liberty or security of an individual unless there is demonstrable need to do so. Further, where there is compelling evidence of such need, the law or other action of the state should be tailored such that the restriction on, or interference with, individual rights is no greater than is necessary to accomplish the objective of the law or state action. *

18. Any new legislation should specifically address privacy issues wherever individual privacy is at risk - general references to the *Charter* and the *Personal Information Protection and Electronic Documents Act (PIPEDA)* are insufficient. *

19. The Internet is a widely-used meeting place for the exchange of political, religious and cultural views as well as a personal communications network. These proposals therefore threaten not only Canadians' right of privacy protected by section 8 of the *Charter* but also the fundamental freedoms of expression and association protected by section 2 and the right to liberty protected by section 7. *

20. Evidence derived from US law enforcement agencies suggests that technological and administrative impediments - more than legal ones - are the cause of most difficulties experienced in cybercrime investigations and prosecutions. Challenges include insufficient record keeping by CSPs,

inability to effect data preservation extraterritorially, inability to crack encryption and a lack of common data sharing protocols. *

21. If law enforcement has difficulty in dealing with new communications technologies, the solution is not to lower the legal standard for interception or search and seizure; rather it is to provide law enforcement agencies with the technical expertise and equipment they need to deal with the evolving environment. *

22. Privacy protection for electronic communications should be *stronger* than that for non-electronic communications, given the unprecedented opportunities available for law enforcement surveillance and intrusion. *

23. Applications for authorization and actual intercepts executed in Canada have decreased over the past twenty years.[39] No explanation is offered for this fall and no statistics are provided on frequency of interception authorizations or how many were abandoned for lack of technical capability to implement them. *

24. The fact that a proposed law may benefit law enforcement agencies does not end the debate about whether the law is constitutional or otherwise desirable. Instead it serves as the beginning of the discussion. *

25. Oversight of any new powers is required. There should be one oversight mechanism with tight rules and judicial supervision - not a proliferation of processes. *

26. The tension between privacy and security is not a zero-sum game. Thinking it is, concedes too much to those who assert that law enforcement should be empowered at any cost. A responsive legislature would seek creative solutions that accommodate both the values of security and those of privacy. Only by engaging in strong oversight of law enforcement action will Canada continue to embody the ideals of the *Charter*. *

**B. REQUIREMENTS TO ENSURE INTERCEPT CAPABILITY**

1. The government has failed to present evidence that this massive surveillance infrastructure is necessary. For example, it is unknown how many investigations have actually been seriously hampered by lack of technical capability. ****

2. Increased powers are not needed for Internet interception in Canada. Existing laws provide ample authority to investigate criminal use of the Internet when police are able to satisfy a judge that there is probable cause for doing so. ***

3. If the proposed intercept capabilities are only required "when a significant upgrade is made to their systems or networks", ISPs may be reluctant to upgrade their operations or capabilities. This could limit the introduction of new and improved services and possibly conflict with Canadian telecommunications policy.[40] ***

4. Most of the challenges faced by law enforcement and national security agencies in accessing modern telecommunications would be more appropriately addressed in Silicon Valley than in Parliament, Congress or Brussels. **

---

[39] Department of Justice presentation at the Ottawa roundtable meeting on lawful access, held on October 21, 2002 - cited by respondent.

[40] Section 7 (g) -*Telecommunications Act* - Statutes of Canada, Chapter 38 - cited by respondent.

5. Canada should be careful to consider how data communications differ from POTS[41] and how law enforcement agencies should treat those differences. This area has caused serious difficulties for the US and the Netherlands when drafting lawful access legislation.**

6. If judges authorize police to monitor private communications, the lack of technical capability should not be such as to frustrate that authorization. *

7. In addition to presuming communications media neutrality[42] with no demonstrated basis for doing so, the consultation document ignores an important corollary - the doctrine of technological neutrality.[43] *

8. For intercepted material to be useful, law enforcement agencies need to understand its content. Serious criminals can make this difficult to do by using readily available strong encryption. This means that criminals, terrorists and other minorities who use encryption for all networked communications will be the only ones who enjoy guaranteed privacy online. *

9. Are private sector service providers agents of the state? Is information collected by CSPs subject to the unreasonable search and seizure provisions of the *Charter?* Neither of these questions is addressed in the consultation document. *

### C. FORBEARANCE

1. The circumstances under which a forbearance order may be justified should be stated, as well as the criteria that will be used to evaluate when, and for how long, such orders will be valid. Any rules or standards dealing with forbearance power should be clear and transparent. *

2. Lawful access requirements are particularly onerous for small ISPs and non-profit organizations providing Internet services to their members. Forbearance proposals are not comforting as they may be discontinued in the future. *

### D. COSTS

1. The proposals require Canadians or their CSPs to pay for the surveillance. This is wrong in principle and impracticable in operation. *

2. The federal government should provide financial support for Canada's ISPs that need to install additional technical facilities to meet the requirements for data preservation. *

3. The increased costs of providing interception capacity and support would severely impact regional freenet service providers which depend on volunteer effort and donations to keep going. *

### E. GENERAL PRODUCTION ORDERS

1. The job of ISPs is to provide services for their customers. This should not include monitoring them for the purposes of the state. Production orders must not be used to circumvent the high

---

[41] Plain Old Telephone Service

[42] All communications media (wireline, e-mail, wireless, etc.) treated similarly under the law - definition provided by respondent.

[43] Technological neutrality is a way of drafting laws and regulations without referring to a particular technology. This is intended to reduce the need for subsequent revision to keep up to date with technological change - definition provided by respondent.

thresholds that would be required if the law enforcement agency were carrying out the search or interception itself. ***

2. The *Criminal Code* should be amended to include a provision for a general production order. This order, however, should only be used for facilitating access to information from CSPs. *

3. There is opposition to the creation of general production orders without clear evidence being presented showing how existing warrant powers are insufficient. If general production orders are nevertheless created, they should be subject to the same procedural safeguards as search warrants (or interception, where appropriate). *

4. For all intents and purposes, production orders are warrants and must be subject to all the thresholds and protections contained in Part XV of the *Criminal Code* and established jurisprudence. The federal government provides no information to show why a widening of such powers is necessary, or why the present search warrant combined with an assistance order is inadequate. *

5. In the same way, it is hard to see how anticipatory orders would require a different standard than that in use at present for search and seizure or interception of communications. *

6. Since law enforcement agencies can use other means to obtain this type of electronic information and, in the event of exigent circumstances, the courts can assist with a court order, it seems unnecessary to give further consideration to the proposed changes. *

7. All interception and/or search and seizure of electronic communications should require judicial approval, should identify a specific target, should identify specific information to be intercepted/ seized and should have a specific rationale and justification for the interception or seizure. All orders issued should be time-limited. *

8. General production orders, if enacted, should require terms safeguarding the confidentiality and security of the information gathered for production. *

9. Today's search and seizure legislation requires the subject of a search or interception to be notified after the fact. Any production order standard should incorporate the same requirement. *

10. A general production order should not be a stand-alone order. It should only be issued if a search warrant or authorization to intercept has already been approved. *

11. The routine use of advanced communications services by the public has led to the perception that these communications are private and not open to examination by law enforcement agencies unless reasonable grounds have arisen. The courts should be the ultimate arbiter of the standard of proof required to protect the privacy of the individual. *

12. A Canadian search warrant by itself cannot be executed outside Canada to obtain documents that are not within the country. Mutual legal assistance procedures are needed to secure offshore documents. Production orders would effectively circumvent this procedure and the protections it provides for those within and outside Canada. *

13. A production order should not be available to compel suspects to participate in an investigation against themselves through the production of information. Such an order would very likely contravene *Charter* guarantees against self-incrimination. *

## F. SPECIFIC PRODUCTION ORDERS FOR TRAFFIC DATA

1. The government is strongly urged to reject any legislation that would allow law enforcement agencies to obtain traffic data under a reduced standard. The proposal portrays traffic data as having little privacy value, arguing that it should be subject to the same reduced standard that applies to Dialled Number Recorders (DNR). Traffic data reveals substantially more about individual activity than DNR information. **

2. Since it seems that law enforcement investigatory tools cannot reliably separate content and traffic data, both types of data should be provided the same level of constitutional protection. **

3. If privacy of the individual is to be protected, we cannot afford to wait to vindicate it only after it has been violated. This is inherent in the notion of being secure against unreasonable searches and seizures[44]. **

4. The existing provisions for collection of telephone-related information in section 492.2 of the *Criminal Code* should be amended to include traffic data, rather than creating a specific production order for this purpose. Traffic data should be limited to Internet addresses, e-mail addresses and routing information. *

5. Jurisprudence has seen the collection of DNR data without judicial approval ruled as both contravening Part VI of the *Criminal Code* and not doing so. This shows that DNR lies in the grey zone and that orders to collect traffic data should always require judicial oversight. *

## G. CNA/LSPID INFORMATION

1. The creation of a national database of any personal information - even limited to CNA information - raises the potential for misuse and should therefore be avoided. It amounts to collection by the state of personal information prior to the commission of an offence or the likelihood of an offence taking place. ****

2. The consultation document fails to provide satisfactory evidence that law enforcement agencies are experiencing pressing difficulties that would justify either the specific production order for customer name and address and local service provider identification (CNA/LSPID) information or the establishment of a national database of subscriber information. ***

3. The following Canadian Radio-television and Telecommunications Commission (CRTC) test for LSPID disclosure by Bell Canada is appropriate and should be adopted for other Canadian CSPs[45]:

> A law enforcement agency must show its authority to obtain the information and indicate that:
>
> - It has reasonable grounds to suspect that the information relates to national security, the defence of Canada, or the conduct of international affairs.
> - The disclosure is requested for the purpose of administering or enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing or administering any such law; or
> - It needs the information because of an emergency that threatens the life, health or security of an individual, or the law enforcement agency otherwise needs the information to fulfill its obligations to ensure the safety and security of individuals or property.
>
> ***

[44] *R v. Dyment* [1988] 2 S.C.R. 417, note 1 at para 23 - cited by several respondents.
[45] Telecom Decision CRTC 2002-12, 12 April, 2002, para. 22.

4. Just because some CNA information is available in directories, does not mean that law enforcement agencies should be granted unimpeded access to CNA information about subscribers who choose to protect their privacy. These individuals have a high expectation of privacy. ***

5. Internet address information should certainly not be accorded a lower standard of access given that the ability to link such information to identified individuals would permit the collection of a vast amount of personal information. ***

6. CSPs should not be obliged to collect subscriber information that they do not already collect in the normal course of their business. This proposed obligation would likely impact most service providers and retailers selling prepaid and other anonymous telephone cards and phones. As noted by the Privacy Commissioner of Canada[46], this would be a gross invasion of privacy and present significant opportunities for data leakage or loss (and subsequent threats, such as identity theft). ***

7. A judicial order should be necessary to authorize law enforcement and national security agencies to obtain information about a subscriber or his/her service provider when carrying out an investigation in relation to the individual concerned. **

8. We should not impose any higher burden on or afford any lesser protection to service providers, retailers and end-users just because they wish to avail themselves of technological solutions as an alternative to Canada Post. *

9. National databases create a single point of vulnerability for those interested in unauthorized access to valuable personal information. A database of this kind would also constitute a blatant contravention of the *Privacy Act* - notably sections 4, 5 and 7.[47] *

**H. DATA PRESERVATION ORDERS**

1. Preservation orders do not exist at present in Canadian law. No data has been provided to justify the creation of this new order, which amounts to a limited form of data retention - except the provisions of the *Convention on Cybercrime*. The proposal to create preservation orders should not be adopted without clear justification. *****

2. This order is a step towards the longer-term data retention scheme adopted in other jurisdictions (such as the UK). It could be used as a "back door" method of obtaining judicial authorization for access, circumventing the higher thresholds which would apply for standard warrants. In any case, this order would represent an expansion, rather than the maintaining of existing lawful access capabilities and should be rejected on that basis alone. ***

3. In the event that preservation orders become law, they should be time-limited, require protection of the confidentiality and security of the preserved data and prohibit the disclosure of the data until a judicial order for production is obtained. ***

**I. VIRUS DISSEMINATION**

1. The legitimate activities of individuals and companies, which possess viruses for analytical research, design, educational or anti-virus purposes, should not be prohibited. Equally, a person found to have an undetected virus or other device residing in their computer without their knowledge should not be found guilty of an offence. **

---

[46] Comments on *Lawful Access Consultation Document*, November 25, 2002 - cited by respondent.
[47] R.S.C 1985, c. P-21 - cited by respondent.

2. Prohibition against viruses, as contemplated by the government, is generally supported. Care must be taken, however, to appropriately define a virus as distinct from a non-deployed or contingent virus. *

## J. INTERCEPTION OF E-MAIL

1. E-mail should receive the same treatment by the Canadian government as first-class mail, affording it the same protection as any other private communication. Thus the statutory and common law rules of evidence would apply equally to e-mail as to postal mail. *****

2. The *Criminal Code* should be amended to clarify that e-mail, at least while in transit, constitutes a "private communication" under section 183. It would then be subject to the same procedural safeguards as all other interceptions under this provision. ***

3. The *Criminal Code* should define clearly when an e-mail ceases to be a communication subject to interception and when it becomes a document subject to search and seizure.[48] **

4. Canadians have a similar reasonable expectation of privacy when using e-mail as they do with other forms of communication. The legal treatment of e-mail should not be determined by technological capability but rather by our values as a society. If we wish to communicate privately by e-mail we should construct our laws to make it so. *

5. Non-profit ISPs run by community associations that offer confidential e-mail lists to enable lawyers to consult with community advocates on difficult cases, law reform issues and other sensitive matters are concerned that the proposed legislation may violate the privacy of advocates and others using this service. *

6. Although ISPs are private companies, they should be subject to state-imposed regulation because they are responsible for the essential service of e-mail delivery. *

## K. OTHER TOPICS INTRODUCED BY RESPONDENTS

### Extraterritorial Issues

1. Cooperation with other states and transmission of intercepted and seized data under mutual legal assistance treaties raises serious sovereignty issues, as well as the potential for jeopardizing *Charter*-protected rights. Dual criminality is a particular issue and Canada must protect its citizens according to Canadian law. *

2. There are serious concerns that Canadians may risk becoming subject to non-Canadian laws based on a cooperation request from another jurisdiction. Canadian law enforcement officials should only enforce Canadian laws and not assist in the enforcement of foreign laws that are substantially different. *

[48] For example, if the e-mail has already been seen by the recipient but it remains stored at the ISP, it is possible that lawful access might represent a seizure rather than an interception.

# CHAPTER 7: COMMENTS BY THE GENERAL PUBLIC [49]

**Total Number of Written Submissions Received: 219**

Where possible the language used in submissions from the general public has been retained to provide the reader with an authentic sense of the comments received.

The number of stars allocated to each item provides an indication of how frequently respondents expressed that opinion or one similar to it. Five stars denotes "very frequently". One star generally indicates a single response on the topic.

## A. GENERAL

1. The opportunity to comment on these proposals is much appreciated. *****

2. It is not clear that the proposals would contribute in any meaningful way to combating crime or terrorism. No solid case has been made to show how access to an individual's online activities can contribute to those objectives either. ****

3. The costs are high, the risks are high and it is not clear what benefit is to be gained from the proposed legislative changes that does not already exist in the law today. ***

4. An outside observer may wonder whether reference in the consultation document to the *Convention on Cybercrime* is more a rhetorical prop than a guiding justification for the proposals introduced.***

5. It is a matter of serious concern when international treaties such as the *Convention* are signed without democratic consultation and then presented to the public as though it is essential that they be ratified. **

6. The consultation document fails to show how the Internet has "created difficulties for investigators". Also, in the case of the Internet, the "need for sophisticated equipment" seems to boil down to packet sniffers which are widely used by ISPs and available for a few thousand dollars. *

7. When the Privacy Commissioner of Canada condemns proposals, they should immediately be withdrawn. *

8. This proposed update to the law is a bad example of the government overstepping the *Canadian Charter of Rights and Freedoms* "in order to protect the people". We do not need to be protected like this. It would be better to live in fear than have rights and freedoms taken away by those (the government) who are supposed to be protecting them. *

9. No case is made in the consultation document that Canadians deserve less privacy when using digital communication rather than analog electronics, or indeed when they use electronics rather than pen and ink. *

10. The privacy and security of the online individual is at much greater risk from other online criminal activity such as identity theft and database break-ins, and inappropriate service provider conduct, than from any other source. *

[49] Includes individuals working for corporations, universities and other organizations who submitted responses, but did not indicate that their submissions were on behalf of their employers.

11. The definition of "service provider" should be refined, so that home networks are excluded, for example. *

**B. REQUIREMENTS TO ENSURE INTERCEPT CAPABILITY**

1. The consultation document claims that ISPs currently do not have the means to allow law enforcement to attach interception equipment. This is false. Virtually all network traffic can be intercepted right now with the right equipment. ***

2. Data encryption is widely used by criminals and terrorists when communicating over private and public networks including the Internet. Encryption techniques are often not detectable, not interceptable and can render law enforcement and ISP interception technology ineffective. ***

3. Anonymous Internet browsing is feasible and endorsed by the World Wide Web Consortium (W3C), the Internet Engineering Task Force (IETF), the Third Generation Partnership Project (3GPP) and other standards-related organizations. Anonymizer clouds on the Internet can also render interception technology useless. ***

4. If the access requirements placed on first level ISPs are too onerous, they will prevent the development of small providers in rural areas and could drive all small ISPs out of business. ***

5. Purposely opening a security hole for law enforcement access in an ISP network is very hard to justify. Suppose it were hacked and data stolen or identity fraud takes place. Who would be liable? Server logs should be plenty good enough for tracking down wrong doings. **

6. The expectation that each ISP be appropriately equipped with the capability to provide a non-specific suite of statistical, interception and log information on a suspect is entirely too open-ended and quite likely too costly for implementation. It would be more practical to have ISPs cooperate with investigative agencies on methods to attach interception, seizure and logging equipment to the service in question. *

7. No legislation should be introduced that enforces a formal system of data interception points throughout Canada's communications infrastructure. Such a system is prone to abuse - especially where packet and cell-switched networks are involved. *

8. It is reasonable to allow the same or equivalent interception capabilities on the Internet that are presently available for regular mail and the telephone service. No more, no less. *

9. Some practical capability solutions:

a. Ensure all Internet e-mail is intercepted/interceptable by the state and (where needed) recorded.

b. Set up a system for obtaining court orders for either the surrender of encryption keys or the installation of keyboard sniffers.

c. Make sure that national security agencies that intercept and (attempt to) decrypt traffic without the knowledge of the sender/receiver are tightly controlled by the courts and a truly independent watchdog.

*

### C. FORBEARANCE

1. It is completely unnecessary to identify CSPs specifically who are exempt from compliance.[50] The procedural laws governing lawful search and intercept should account for this. Exceptions should be granted or not by the judge evaluating an order. *

### D. COSTS

1. Should a law enforcement agency require assistance from a CSP that is beyond the normal cost of doing business for that provider, then the agency should pay the cost of the assistance. Such costs should not be the responsibility of the service provider nor should they be passed on to the CSP's end client. ***

2. Costs incurred by agencies carrying out interception and monitoring online and on other parts of the network should be reported annually to Parliament and made available to the Canadian public. *

3. Because of the potentially random, unpredictable nature of law enforcement investigations, the cost and tools associated with police seizure or interception should be borne by the law enforcement agency - not the service provider. *

4. Fair financial compensation for ISPs should include direct labour costs for law enforcement cooperation, the opportunity cost of not being able to use the staff involved for other chargeable tasks, capital expenditure on hardware, software, licences and maintenance costs. *

### E. GENERAL PRODUCTION ORDERS

1. No ISP should be an information collection agency on behalf of the Canadian government. If the government wants and needs information, it should be responsible for retrieving, collecting and storing it. The ISP should only be obliged to provide the facilities when there is a lawful order to do so. ****

2. Production orders are unnecessary, given the ability of law enforcement agencies to obtain information using existing means. The rationale presented for issuing anticipatory orders is absurd. ***

3. Any attempt to monitor communications must be authorized by court order. The request for such an authorization must be explicit in terms of who, what, where and when (including for how long to monitor). Such a request should not be open-ended and should not exceed a maximum period defined in legislation. One month might be a suitable limit. ***

4. Production orders need to be explicit and precise. Wild goose chases should be specifically prohibited. **

5. Law enforcement agencies should not be able to monitor private transactions without judicial oversight by way of an anticipatory order. **

### F. SPECIFIC PRODUCTION ORDERS FOR TRAFFIC DATA

1. It is unacceptable for police to require ISPs to keep a log of websites each individual has visited, in case they desire to snoop later on. Individuals should not be investigated, or deemed suspicious, based on their choice of channels or reading matter, online or offline. *

[50] Public identification of exempt service providers shows criminals where the safe havens are.

2. E-mail headers tend to include much more information than a postal envelope. They will typically include not just the addressee but also the source, subject and size of the message. *

**G. CNA/LSPID INFORMATION**

1. Another national database of personal records is completely unnecessary. There is no national registry of telephone users or postal mail users - there should not be one for Internet users. A national database of this kind would also be a dangerous accumulation. Can bureaucrats guarantee that this highly sensitive database would never be successfully hacked? *****

2. There is no national registry of telephone users or postal mail users - there should not be one for Internet users. That is a completely unacceptable suggestion.****

3. A national database of this kind would be a dangerous accumulation. Can bureaucrats guarantee that this highly sensitive database would never be successfully hacked? **

4. The consultation document makes it clear that this type of order is required to allow law enforcement agencies to carry out "fishing expeditions" in the absence of justification for a court order. Judicial oversight is essential. *

5. CSPs should not be required under any circumstances to collect information that they would not normally collect in their day-to-day operations. Doing so could interfere with legitimate business models that rely on not collecting such information, add costs and would result in taking on work that law enforcement agencies should be doing themselves. *

6. Severe penalties should be established for unlawful access to ISP databases containing individuals' online activity records and other personal data. *

**H. ASSISTANCE ORDERS**

1. Assistance orders should be explicitly required rather than implied. They should detail clearly the assistance required. *

2. Rate schedules for assistance to law enforcement agencies should be similar to those charged by the government for responding to *Access to Information Act* requests from the public. *

**I. DATA PRESERVATION ORDERS**

1. Data preservation orders should apply to all forms of data regardless of medium. They should be valid for no longer than is reasonable to secure the necessary production order - like one week. ***

2. The proposed preservation of e-mails and other Internet communication for use by law enforcement agencies is bound to increase the use of cryptography software by the public. **

**J. VIRUS DISSEMINATION**

1. The *Convention* would make it illegal for software companies to create or store viruses and it would make university researchers and ISPs criminals for studying virus behaviour. This is unreasonable. *****

2. The subject of criminalizing virus software should be revised to include all types of malicious software - software (or devices) developed or possessed with the *intent to infringe* on the integrity, availability and confidentiality of computer systems and telecommunications networks. ***

3. Under the present provisions of the *Criminal Code* only the effects of spreading a computer virus, or an attempt to do so, are criminal acts. There is no need to change the existing law. ***

**K. INTERCEPTION OF E-MAIL**

1. E-mail, like snail mail and telephone conversations should be treated as private communications. Legislation arising from this consultation should plainly codify the expectation of privacy except when information is publicly disseminated. *****

2. E-mails should require a court order for interception regardless of the point of interception. ****

3. Intercepting an e-mail while stored at an ISP is equivalent to intercepting a telephone message recorded at a local switch on a facility like Bell's Call Answer service. It is a private communication and should always be treated as such. **

4. Obliging ISPs to retain e-mails for up to six months raises serious questions. What guarantee does the public have that their emails will actually be deleted after six months and how will the government guarantee that ISP employees will not abuse the records of e-mails at their disposal? *

5. Technical detail should be avoided in any future legislation about e-mail interception as it may open the door to legal wrangling and unnecessary litigation. *

6. Care should be taken to ensure that - in addition to e-mail - newer communications facilities such as real-time chat and messaging services are included in any subsequent legislation. *

# ANNEX A:

# LAW ENFORCEMENT AGENCIES AND ASSOCIATIONS RESPONDING TO THE CONSULTATION

| | Law Enforcement Agencies and Associations |
|---|---|
| 1 | Abbotsford Police Department |
| 2 | Barrie Police Service |
| 3 | Brantford Police Service |
| 4 | Brockville Police Service |
| 5 | Calgary Police Service |
| 6 | Canadian Association of Chiefs of Police |
| 7 | Charlottetown Police Department |
| 8 | Chatham-Kent Police Service |
| 9 | CN Police |
| 10 | Criminal Intelligence Service Alberta |
| 11 | Département de police de la ville de Laval |
| 12 | Durham Regional Police Service |
| 13 | Edmonton Police Service |
| 14 | Greater Sudbury Police Service |
| 15 | Guelph Police Service |
| 16 | Halton Regional Police Service |
| 17 | Hamilton Police Service |
| 18 | Lethbridge Police Service |
| 19 | London Police Service |
| 20 | New Liskeard Police Service |
| 21 | Niagara Regional Police Service |
| 22 | Oak Bay Police Department |
| 23 | Ontario Provincial Police |

| | |
|---|---|
| 24 | Ottawa Police Service |
| 25 | Oxford Community Police |
| 26 | Peterborough Lakefield Community Police Service |
| 27 | RCMP – Calgary |
| 28 | RCMP - Edmonton |
| 29 | RCMP – Halifax |
| 30 | RCMP – Kelowna |
| 31 | RCMP – London |
| 32 | RCMP – Montreal |
| 33 | RCMP – New Brunswick |
| 34 | RCMP – Ottawa |
| 35 | RCMP – Prince Edward Island |
| 36 | RCMP – Quebec City |
| 37 | RCMP – Red Deer |
| 38 | RCMP – Strathcona County Detachment |
| 39 | RCMP – Toronto |
| 40 | RCMP – Vancouver |
| 41 | RCMP – Whitehorse |
| 42 | Régie intermunicipale de police – Vallée du Richelieu |
| 43 | Regina Police Service |
| 44 | Royal Newfoundland Constabulary |
| 45 | Saint John Police Force |
| 46 | Saskatoon Police Service |
| 47 | Sault Ste. Marie Police Service |

| | |
|---|---|
| 48 | Sûreté municipale de Mont-Tremblant |
| 49 | Thunder Bay Police |
| 50 | Timmins Police Service |
| 51 | Toronto Police Service |
| 52 | Truro Police Service |
| 53 | Vancouver Police Department |
| 54 | Waterloo Regional Police Service |
| 55 | Weyburn Police Service |
| 56 | Winnipeg Police Service |

# ANNEX B:

## COMPANIES AND INDUSTRY ASSOCIATIONS RESPONDING TO THE CONSULTATION

| | Companies |
|---|---|
| 1 | Aliant Telecom Inc.<br>BCE Inc. (Bell Canada Enterprises)<br>MTS Communications Inc.<br>Saskatchewan Telecommunications |
| 2 | Microcell Telecommunications Inc. |
| 3 | Rogers Wireless AT&T |
| 4 | Telesat Canada |
| 5 | Telus |
| 6 | VeriSign Inc. (US) |
| 7 | Yahoo! Canada |

| | Industry Associations |
|---|---|
| 1 | Association des compagnies de Téléphone du Québec |
| 2 | Canadian Advisory Committee – Information Technology Security |
| 3 | Canadian Association of Internet Providers |
| 4 | Canadian Bankers Association |
| 5 | Canadian Cable Television Association |
| 6 | Canadian Chamber of Commerce |
| 7 | Canadian Information Processing Society |
| 8 | Canadian Public Policy Committee of the Computing Technology Industry Association |
| 9 | Canadian Wireless Telecommunications Association |
| 10 | Information Technology Association of Canada |
| 11 | Ontario Telecommunications Association |
| 12 | US Internet Service Providers Association (US) |

# ANNEX C:

## PRIVACY AND INFORMATION COMMISSIONERS RESPONDING TO THE CONSULTATION

| | Privacy and Information Commissioners |
|---|---|
| 1 | Privacy Commissioner of Canada |
| 2 | Commission d'accès à l'information du Québec |
| 3 | Information and Privacy Commissioner, Ontario |
| 4 | Office of the Information and Privacy Commissioner, Alberta |
| 5 | Office of the Information and Privacy Commissioner for British Columbia |

# ANNEX D:

## CIVIL SOCIETY GROUPS RESPONDING TO THE CONSULTATION

| | Civil Society Groups |
|---|---|
| 1 | B.C. Civil Liberties Association |
| 2 | British Columbia Freedom of Information and Privacy Association |
| 3 | Canadian Bar Association |
| 4 | Canadian Civil Liberties Association |
| 5 | Canadian Library Association |
| 6 | Civil Liberties Association, National Capital Region |
| 7 | Electronic Frontier Canada and Electronic Frontier Foundation (US) |
| 8 | Electronic Privacy Information Center (US) |
| 9 | Internet Law Group - University of Manitoba |
| 10 | Option consommateurs |
| 11 | PovNet |
| 12 | Privaterra - Computer Professionals for Social Responsibility |
| 13 | Public Interest Advocacy Centre |
| 14 | Vancouver Community Network |

# ANNEX E:

## GOVERNMENT DEPARTMENTS RESPONDING TO THE CONSULTATION

| | Government Departments |
|---|---|
| 1 | Alberta Justice |
| 2 | Alberta Solicitor General |