Lawful Access Consultation

Response of the

Canadian Wireless Telecommunications Association

submitted to

Department of Justice
Industry Canada
and
Solicitor General Canada

December 16, 2002

Introduction

1. The Canadian Wireless Telecommunications Association ("CWTA") has carefully reviewed the Lawful Access Consultation Document (Consultation Document), issued by the Department of Justice, Industry Canada and the Solicitor General Canada on August 25, 2002.

2. CWTA is the authority on wireless issues, developments and trends in Canada. It represents cellular, PCS, messaging, mobile radio, fixed wireless and mobile satellite carriers as well as companies that develop and produce products and services for the industry.

3. This response to the Consultation Document contains an overview of the key issues identified by the CWTA and several sections organized to mirror the sections contained in the Consultation Document followed by a Conclusion.

Overview

4. The CWTA recognizes that lawful access is an important tool for national security and law enforcement. The services provided by wireless carriers also serve important objectives of federal telecommunications policy. The CWTA understands that the impetus behind the review of the legislative framework for the provision of lawful access to communications is tied to the Council of Europe Cybercrime Convention.

5. We would like to provide constructive comments regarding the proposal but our ability to do so is limited at this time. While the Consultation Document provides a somewhat helpful high-level overview of the issues at hand, a number of critical questions remain unanswered regarding the proposals contained in the document. In order to provide meaningful comment on the policy proposals, service providers must understand the requirements that they will be expected to meet under the new legislation. These detailed requirements are not included in the Consultation Document.

6. In a letter to the Minister of Justice dated November 1, 2002; CWTA requested that draft legislation as well as any accompanying regulations be provided for public consultation. After further review of the Consultation Document and the issues, CWTA is now of the view that a further round of consultation is warranted.

7. The CWTA strongly suggests, therefore, that prior to any draft legislation being presented to Parliament, the Departments should provide a second

public consultation paper containing the details absent from the current document. The CWTA and its members need to better understand the entire operational framework of the lawful access proposal.

8. The entire operational framework will, of necessity, be very complex. It will impact several *Acts* of Parliament and will involve all three levels of government. Only after the entire framework is understood will the CWTA be able to ascertain all of the various impacts that the proposed legislation will have on the wireless telecommunications industry. In this regard, the CWTA notes that the submission of the Privacy Commissioner of Canada repeatedly expresses concern over the lack of critical details in the Consultation Document.

9. The CWTA also proposes that the new requirements not take affect immediately on the day the new legislation comes into force. A period of time will be required during which service providers and vendors alike will come to fully understand the new requirements and enable the service providers to make the required network modifications to meet the basic intercept capability. It is the view of the Association that the suggested grace period is a very positive and pragmatic proposal. None of the stakeholders to the lawful access initiative, including law enforcement, government, service providers nor Canadian citizens, would benefit from the introduction of new and immediate requirements if the technology to meet the new requirements in unavailable.

10. Moreover, as indicated in the Consultation Document, much of the impetus for the proposed legislation stems from the Council of Europe Convention on Cybercrime. The CWTA understands that the European Community itself continues to develop specific regulations. Accordingly, it would be prudent for Canada to undertake a further consultation once the details of the European regulations are known.

11. A number of elements within the current proposal may have significant impacts on the manner in which wireless carriers conduct their business and may significantly increase the cost of doing so. The CWTA is opposed to any new obligations, such as validation of customer information, that would require a radical and costly overhaul of wireless carrier business processes and services. CWTA is also opposed to any obligation that might cause the elimination of certain services or class of services, such as prepaid wireless. Law enforcement and security interests must be fairly balanced with the interests of the communications industry and wireless consumers.

12. A transparent process is required that would clearly articulate the requirements for compliance that must be met by all carriers. All service providers competing in the same market should face the same

requirements to provide the same level of lawful access to communications. At the same time, regulations or standards must be flexible enough to accommodate the different technologies employed by wireless carriers.

13. Significant hardware systems and software upgrades may be required in order to comply with any new lawful access standards that may result from the passage of new legislation. The CWTA is opposed to the imposition of proprietary or uniquely Canadian solutions for lawful access. Where new standards are developed, the CWTA strongly endorses the harmonization of such standards with international telecommunications industry standards. An industry standard approach would increase the likelihood that technology vendors will develop and provide technology that satisfies the lawful access requirements. This approach would also likely result in costs that are lower than would be the case if proprietary solutions are required. CWTA notes that these standards will largely be driven by the markets in the United States and Western Europe, areas that are also moving to ratify the Convention on Cybercrime.

14. The new legislative framework must recognize that the benefits associated with lawful access accrue to all Canadians and therefore it is Government that must provide the financial resources to pay for the network modifications necessary to meet the lawful access requirements. Regardless of whether or not retrofitting is required, the tools and equipment to provide lawful access will represent a significant incremental cost to industry; one that industry cannot bear alone. Moreover, any future modifications of the standard would require additional financial commitment by the government.

15. The final concern to be emphasised in this overview pertains to service provider liability in the provision of lawful access. The CWTA is of the view that the new law must not leave service providers open to legal actions by customers or others for the mere provision of lawful access. Accordingly, the new legislation should provide appropriate safe harbour liability protection provisions for service providers.

Current Provision of Lawful Access

16. As noted in the introduction to the Consultation Document, certain providers of wireless services have been required to have facilities capable of lawful access pursuant to conditions of licence imposed under the *Radiocommunications Act*. Contrary to the apparent view of some law enforcement / government stakeholders, however, the lawful access proposal will nonetheless impose significant new obligations on wireless carriers with respect to packet-switched services. While the current

conditions of licence do not detail the specific obligations of wireless carriers, the conditions do require that carriers adhere to the requirements of the Solicitor General. The Solicitor General has, in turn, developed a document that outlines the enforcement standards for lawful interception of telecommunications (often referred to as the Solicitor General's 23 Standards).

17. The 23 Standards were developed in an era of circuit-based switching and can only reasonably be interpreted to apply to services offered using circuit-based switching. The CWTA strongly disagrees with any and all assertions that the Solicitor General's 23 Standards apply to services offered using packet-based switching. Various policy documents from the Department of Industry provide reference for CWTA's position:

    a. PCS Spectrum Licence Condition 11 states "Licensees using the spectrum for circuit-switched voice telephony systems must, from the inception of service, provide for and maintain lawful interception capabilities as authorized by law".

    b. The *Policy & Licensing Procedures for the Auction of Additional PCS Spectrum in the 2 GHz Frequency Range* (DGRB-005-00/DGTP-007-00, June 2000) states "The Department notes that the Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications were written to apply to circuit-switched voice telephony systems and as such, the standards are not readily applicable to a packet-based environment using routers rather than traditional switches...the Department will only incorporate compliance with the Solicitor General's current standard for circuit-switched voice telephony systems."

    c. In the Policy and Licensing Procedures of both MCS at 2500 MHz (DGRB-006-99) and the Auction of the 24 and 38 GHz Frequency Bands (DGRB-003-99/DGTP-005-99) the Department chose not to "incorporate compliance with the Solicitor General's current standard into a licence condition at this time" because the services were not anticipated to provide circuit-switched voice applications.

18. Further, it is unclear, in our view, as to what will happen to the existing conditions of licence and the Solicitor General's 23 Standards once new legislation is passed. The CWTA would assume that the new laws would take precedence over the current licensing conditions and would assume further that new regulations would be passed which would be linked directly to the new law.

19. It must also be emphasised that wireless carriers operate a variety of networks using different technologies. These networks are also at various

stages of development and deployment. In this regard, while the Consultation Document suggests that wireless carriers already provide lawful access; in reality not all wireless carriers are at the same level of compliance with the Solicitor General's 23 Standards. The question therefore arises as to whether the relevant state of compliance with the 23 Standards will be entrenched with the new law?

20. The CWTA therefore recommends that existing conditions of licence pertaining to the provision of lawful access be rescinded once the new law is in force. CWTA further recommends that all forbearance conditions currently in-place, should be continued over and remain in force for a reasonable period under the new legislation.

21. The CWTA is strongly of the view that it is the responsibility of Government to pay for all costs associated with the provision of lawful access. If the Government accepts this responsibility, then the need to maintain the existing forbearance decisions will become moot. In addition, the use of Government resources will enable the application of identical requirements to all carriers in a timely and consistent manner.

22. The Solicitor General's 23 Standards and, as a result, the interception capabilities of wireless carriers, deal primarily with the interception of circuit-switched voice and data received or transmitted by a wireless customer. As indicated above, the CWTA is strongly of the view that the Solicitor General's 23 Standards can only be legitimately applied to services offered using circuit-based switching. The Consultation Document, however, with its strong linkages to the European Convention on Cybercrime, suggests a number of requirements pertaining to the Internet that are not detailed in the 23 Standards. As such, the CWTA would anticipate that this aspect of the new law would have a significant impact on the wireless industry. Most wireless carriers offer services and sell devices that will allow customers to send and receive email, as well as browse the Internet over packet-based networks.

23. The CWTA further notes that the Consultation Document alludes to tools such as data retention, prevention of virus dissemination and subscriber and service provider information. These mechanisms are not found in the Solicitor General's 23 Standards and, as such, would have a significant impact on the wireless industry. These impacts are detailed later in this response.

24. The CWTA is opposed to the imposition of requirements that will significantly impact existing services, distribution channels and business processes. These things have been developed by wireless carriers for business purposes including the provision of services, and the collection of revenues. Any information or data that is incidental to these purposes

may or may not be useful to law enforcement and security agencies. The CWTA is not opposed to making such information available in the context of lawful access. However, it is opposed to the notion that carriers will be required to undertake substantial modifications, or to eliminate certain distribution channels or services in order to comply with new lawful access requirements.

Working Definitions

25. The Consultation Document introduces a number of working definitions including “Service Provider”, “Transmission Facility”, “Transmission Apparatus” and “Telecommunications Associated Data”. CWTA is concerned that other fundamental terms such as “Basic Intercept Capability” and “Significant Upgrade” are not defined in the Consultation Document.

26. At the outset the CWTA would note that the definitions provided differ from those provided by the *Telecommunications Act*. In particular, the *Telecommunications Act* contains definitions of “Telecommunications Facility”, “Transmission Facility” and “Telecommunications Service” (as opposed to “Service Provider”). A definition of “Telecommunications” is also provided.

27. Confusion could arise from two *Acts* containing differing definitions. The CWTA recommends that the new law use, where possible, existing definitions contained in the *Telecommunications Act*.

28. In addition, the working definition provided in the Consultation Document for service provider is given as: “means a person who owns or operates a transmission facility that is used by that person or another person to provide telecommunications services to the public in Canada”. This definition omits an entire class of service providers referred to as “resellers”, and also would appear to exclude entities such as technology vendors, enhanced service providers, and application service providers, any of which may own and operate computer servers and/or systems that form an integral part of the services they provide to other service providers such as wireless carriers. Wireless carriers cannot be held liable for data, servers and systems that they do not control.

29. In this regard, the language used in the European Convention may be helpful, “any public or private entity that provides to users of its service the ability to communicate by means of a computer system”, and “any other entity that processes or stores computer data on behalf of such communication service or users of such service.”

30. While in our view the definition of service providers omits several classes of providers, it does appear to capture a number of smaller organizations like hotels, universities and, possibly, coffee shops that operate a transmission facility and offer service to the public. It is also our understanding that some types of service providers might somehow be exempted from complying with the obligation to provide intercept capabilities. Such exemptions, if they materialize, would obviously be a concern from the standpoint of public security but also from standpoint of creating a level playing field for competitors in the communications industry. It would be unjust to require larger licensed service providers to fully comply with the new legislation while exempting smaller competitors from compliance with the new legislation. The CWTA submits that all service providers competing in the same market should face the same requirements to provide the same level of lawful access to communications.

31. The working definition of Telecommunications Associated Data is "means any data, including data pertaining to the telecommunications functions of dialling, routing, addressing or signalling, that identifies, or purports to identify, the origin, the direction, the time, the duration or size as appropriate, the destination or termination of a telecommunication transmission generated or received by means of the telecommunications facility owned or operated by a service provider." It is unclear from this definition whether wireless carriers would be expected to provide the specific location of the customer (assuming location information is available) and whether the carrier would be further expected to update (track) the location information. CWTA notes the Privacy Commissioner of Canada expressed some concern about this idea.

32. The CWTA agrees with the working definitions of Transmission Facility and Transmission apparatus.

Specific Legislative Proposals

33. The following section addresses the specific proposals contained in the Consultation Document as they are presented in the document.

General Requirements

34. As noted earlier, CWTA is extremely concerned that the concepts of "Basic Intercept Capability" and "Significant Upgrade" are not defined in the Consultation Document. This makes it most difficult to provide meaningful comment as to the appropriateness of these concepts.

35. This concern is most pronounced when considered in light of the proposal that service providers would be expected to cover the costs associated with these proposals. If sufficient funding is available from government, the potential impacts of these definitions would be less severe.

36. Nevertheless, the CWTA believes that the mere extension of service areas should not be considered as a significantly upgraded service to the public. Wireless carriers are continually extending the coverage areas of their networks to better serve their customers. These incremental additions, even where they may be geographically broad, do not change the characteristics of the services available but merely allow access to services in areas previously un-served.

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

38. "Core network" should be defined as the physical entities which provide support for the network features and telecommunication services. The support provided includes functionality such as the management of user location information, control of network features and services, the transfer (switching and transmission) mechanisms for signalling and for user generated information.

39. It is worth noting that, whatever the definition, network equipment must be available to provide the capability. The CWTA therefore believes that the date that the requirements of the legislation would come into effect, as proclaimed by the Governor-in-Council, should be a minimum of 12 months after the new legislation comes into force. A period of time will be required during which service providers and vendors alike will come to fully understand the new requirements and enable the service providers to make the required network modifications to meet the basic intercept capability. It is the view of the Association that the suggested grace period is a very positive and pragmatic proposal.

Regulations

40. As noted above, some wireless carriers have experience in providing lawful access to communications. Some of the challenges these carriers faced in the provision of lawful access relate to the regulation-like standards developed by the Solicitor General. The interpretation of these standards has, in some respects, evolved since the conditions of licence were first imposed – causing the wireless carriers to modify their networks and operational procedures in order to remain in compliance with the evolving requirements.

41. The CWTA supports the creation of specific regulations or standards that clearly define what must be done. However, the regulations or standards must be flexible enough to accommodate the different technologies employed by wireless carriers.

42. Moreover, it is the view of the CWTA that the new regulations should not be modified without consultation with industry and without consideration of the cost impact on industry associated with changing the regulations. Additional impacts can occur after changes to regulations if law enforcement agencies don't all modify their own systems, forcing service providers to provide data in more than one format or mode. The regulations should also require law enforcement agencies to upgrade their equipment to accommodate any jointly agreed modifications to standards or methods.

43. While the Consultation Document speaks to adoption of new technologies by service providers, it does not speak to the impact of changes in regulations. Costs associated with changes to the regulations should be the responsibility of government, not industry.

44. The CWTA would further urge that the regulations be consistent with international telecommunications industry standards. This would help to reduce the costs associated with the provision of lawful access. The CWTA is opposed to the notion that proprietary or uniquely Canadian solutions will be imposed on wireless carriers.

45. With regard to fees for the ongoing provision of lawful access, the CWTA is of the view that it is appropriate for carriers to charge fees for the provision of lawful access service. This would be consistent with the approach taken by other jurisdictions.

Forbearance

46. As noted in our comments regarding the definition of service provider, we understand that some types of service providers might somehow be exempted from complying with the obligation to provide intercept capabilities. Such exemptions, if they materialize, would obviously be a concern from the standpoint of public security but also from standpoint of creating a level playing field for competitors in the communications industry. It would be unjust to require larger licensed service providers to fully comply with the new legislation while exempting smaller competitors from compliance with the new legislation.

47. CWTA cannot provide detailed comments on this issue as the concept of exemption is not included in the Consultation Document, and no details have been provided regarding any process that may be used to determine an exemption. The CWTA submits that all service providers competing in the same market should face the same requirements to provide the same level of lawful access to communications.

48. As in the comments on the definitions of "Basic Intercept Capability" and "Significant Upgrade", the concern about ensuring equitable obligations between competitors is most pronounced when considered in light of the proposal that service providers would be expected to cover the costs associated with these proposals. If sufficient funding is available from Government, the market distortions from such exemptions will be minimized.

49. The CWTA believes that any service provider that is unable to meet the basic minimum intercept requirements should be required to seek forbearance.

50. The CWTA supports the proposal that a forbearance mechanism be included in any new scheme.

51. The CWTA wishes to emphasise the importance of a fair and open public process dealing with all requests for forbearance.

Compliance Mechanism

52. The CWTA believes a complaint driven compliance mechanism in which the law enforcement agencies would most likely be the complainant, is the most suitable approach.

53. Given the technical nature of the provision of lawful access service, the CWTA is of the view that the Minister of Industry, through his Department, is the appropriate delegate to determine compliance.

54. The CWTA believes that wireless carriers are currently meeting what will become the basic intercept capability in the new legislation. If it is deemed that a service provider is not meeting this basic capability, then it would appropriate for the service provider to seek forbearance.

55. If forbearance is not granted and prior to the imposition of any penalty, the CWTA strongly believes that service providers should be afforded with a period of time in which to transition from non-compliant state, to a state of compliance. The CWTA recommends a transition period of 12 months.

Costs of Ensuring Intercept Capability

56. Significant hardware and software systems may be required in order to comply with any new lawful access standards that may be developed. The CWTA fully supports an approach whereby new requirements are harmonized with industry standards. This will increase the likelihood that solutions will be made available by a broad range of vendors, and will likely result in lower cost than would be the case for proprietary solutions.

57. The benefits associated with lawful access accrue to all Canadian citizens and therefore it is Government that must provide the financial resources to pay for the network modifications required to meet the lawful access standard, as is the case with other policing and national security costs. Moreover, any future modifications of the standard would require additional financial commitment by the government.

58. The Consultation Paper proposes the following regime governing costs:

    a. *Service providers would be responsible for the costs associated with providing the lawful access capability for new technologies and services, and*

    b. *Service providers would be responsible for the costs associated with providing a lawful access capability when a significant upgrade is made to their systems or networks, however*

    c. *They would not be required to pay for necessary changes to their existing systems or networks.*

59. It would appear that the Departments have proposed this cost regime based on the following assumptions:

    a. that the cost of retroactively-fitting existing systems or networks to provide new lawful access capabilities will be substantial,

    b. that, in comparison to the cost of retro-fits, the cost of incorporating new capabilities into the design of a new system or network from the beginning are usually lower, and

    c. that the costs of incorporating new capabilities into the design of a new system or network, or into a "significantly upgraded" service, are not substantial and are insignificant.

60. CWTA agrees with the assumption that in general, costs associated with retro-fits are significant. CWTA submits however, that although lower than the costs of retrofitting, the costs of incorporating capabilities into new

systems and networks are also significant. Even when services and capabilities are included in a standard package, significant software activation charges must often be paid to the vendor before that service or capability can be activated. Only in time will the cost of incorporating lawful access services or capabilities into new systems or networks become relatively insignificant and therefore will no longer require the application of explicit charges.

61. CWTA submits that service providers should only be responsible for the cost of providing lawful access capabilities in new systems or networks, or in significantly upgraded services, when the cost of doing so is no longer significant and is implicit in the cost of the basic feature package. In other words, public funding should be provided as long as the cost of providing lawful access for existing, significantly upgraded, or new services and networks is significant, and as long as the capabilities in question are only available upon payment of explicit charges.

62. With regard to the ongoing provision of lawful access service to law enforcement agencies, the CWTA believes that the new legislation should enshrine the principle that law enforcement should pay service providers for assistance provided. While the federal law enforcement agencies generally accept this principle, some CWTA members have experienced difficulty recovering their costs in providing the required service to certain local law enforcement agencies.

63. The provision of lawful access services to law enforcement goes well beyond the concept of civic duty on the part of service providers. Providing assistance to law enforcement agencies generates significant ongoing costs in terms of personnel, training, and security requirements in addition to the specific costs of implementing an interception capability.

64. It is the view of the CWTA that an enshrined principle would assist both service providers and law enforcement agencies to arrive at negotiated fee for service arrangements with each other.

65. The CWTA further believes that, in addition to enshrining the principle described above, the legislation should point to the Departments of Industry Canada and Solicitor General as arbitrators to any dispute regarding fee for service between a service provider and a law enforcement agency.

Amendments to the Criminal Code and other statutes

Orders to obtain subscriber and/or service provider information

66. The CWTA strongly opposes the imposition of this obligation beyond those situations where a wireless carrier is already collecting this information. Moreover, the CWTA is of the view that service providers should not be liable for the accuracy of customer name and/or address information. In this regard, the CWTA would note that the European Convention refers to subscriber information *in that service provider's possession or control*.

67. Generally, wireless carriers collect, validate and maintain customer information to the extent that such information is necessary to successfully provide service and to collect payment. For postpaid services (services for which the customer receives a monthly bill), wireless carriers would typically undertake a credit check to determine a prospective customer's ability to make monthly payments for the services provided. However, this process is geared to validating credit worthiness, not customer name and address. Wireless carriers do not undertake exhaustive validation of the information that is provided by customers and wireless carriers do not warrant that such information is valid or correct, or that it would satisfy the requirements of law enforcement and security agencies. Further, wireless carriers are almost entirely reliant on customer initiated notification with respect to address changes.

68. Consequently, the CWTA opposes the imposition of any obligation for service providers to collect information that they are not already collecting for their own purposes. Significant service, business and cost issues would arise if wireless carriers were required to collect, validate and maintain accurate customer information for the purposes of lawful access.

69. First, any such requirement would likely obligate wireless carriers to insist that customers present a minimum degree of official identification at the point of purchase. This would also require that wireless carriers, and the literally thousands of independent distribution agents and outlets they rely on, would be capable of validating such identification. CWTA notes in this regard the concerns raised by the Privacy Commissioner of Canada.

70. Second, an overwhelming issue arises with respect to on-line purchases of a wireless service since, for these purchases, the entire transaction is conducted over the Internet, not in person. Similarly, customers who opt for on-line billing will be billed on-line and will not have a monthly invoice sent to a physical address. If they chose to move, the carrier will have no

means of knowing, apart from the customer taking the initiative to update this information by accessing their on-line account. In the case of purchasing or billing, on-line transactions do not lend themselves to the presentation and validation of the customer's identification. Wireless carriers, and countless other businesses in Canada and abroad, have already made significant investments in on-line purchasing, billing and customer relations capabilities and they rely on this channel as a useful and cost-effective means by which to acquire, bill and interface with their customers.

71. Third, another problem is created with respect to prepaid wireless services provided by wireless carriers since valid customer information is not required by carriers in order to provide prepaid services. Given that a credit check is not required, and that the customer will never receive a monthly bill, there is no need for the carrier to request the customer's name or address. The entire transaction of activating the customer's account can be conducted over the phone and absent any identification. Although wireless carriers are increasingly requesting customer name and address information for business purposes, this information is not validated, nor do carriers deny service if the customer does not provide the information.

72. It should be noted that this situation is not isolated to wireless phones. The verification of a customer's address is only necessary when a service provider must establish a physical connection to the customer. For example; Direct Broadcast Satellite, Multipoint Distribution Service, dial-up Internet Service Providers, and prepaid local and long distance phone card providers are also capable of providing service without knowing the address of the customer.

Assistance Orders

73. As noted earlier, CWTA believes that the new legislation should enshrine the principle that law enforcement should pay service providers for assistance provided. While the federal law enforcement agencies generally accept this principle, some CWTA members have experienced difficulty recovering their costs in providing the required service to certain local law enforcement agencies.

74. It is the view of the CWTA that an enshrined principle would assist both service providers and law enforcement agencies to arrive at negotiated fee for service arrangements with each other.

75. The CWTA further believes that, in addition to enshrining the principle described above, the legislation should point to the dual Departments of

Industry Canada and Solicitor General as arbitrators to any dispute regarding fee for service between a service provider and a law enforcement agency.

Data-preservation orders

76. The CWTA would note that this is another area of the Consultation Document that would benefit from the inclusion of more details. We currently understand that data-preservation in this context means a snapshot of data that a service provider has access to at a point in time. Moreover the order would only apply to data that service providers would ordinarily save during their normal course of business.

77. The CWTA wishes to emphasise that it would be extremely unreasonable to expect service providers to immediately comply with a data-preservation order as soon as the order is served on the service provider. While every effort would be made to expedite compliance with the order, such compliance would not be instantaneous.

78. It is also our understanding that the data-preservation order should only apply to computer data.

79. The CWTA believes that only the courts should be authorized to issue a preservation order.

80. The CWTA recommends that the custodian of data should not be compelled to preserve data any longer than is absolutely necessary. The operational and storage costs associated with preserving data are high. In consultations, the Departments indicated that the majority of data-preservation orders would require that data be preserved only for 2-3 days while the maximum 90 day period mentioned in the Consultation Document would only be required in those cases that require international cooperation. CWTA suggests that the text of the legislation should indicate a shorter “typical” application, while allowing for a longer maximum for international cases.

Other mechanisms to provide subscriber and service provider information

81. CWTA is not convinced that any new mechanism for law enforcement to identify a local service provider is required.

82. The CWTA notes that the Canadian Numbering Administration Consortium Inc. (CNAC) will, in part, respond to these stated needs of law enforcement to link a telephone number to its service provider. As directed

by CNAC, the Canadian Numbering Administrator provides on its website (http://www.cnac.ca/) a listing of NPA–NXX combinations along with the name of the code holder (almost always the service provider) for each. For example, 613–728 is a NPA–NXX combination used in Ottawa–Carleton to provide local telephone service and the code holder is Bell Canada. Anyone who wishes to consult the website is able to freely identify the service provider. This is referred to as the National Numbering Index, or NNI. It is also worth noting that this information is already publicly available, for a cost, from the Telcordia NPA/NXX database.

83. The CWTA also notes that there is an existing Bell Canada tariff which allows law enforcement agencies, under CRTC specified conditions, to access an enhanced NNI which also reflects the impacts of local number portability and can therefore provide the service provider for each line number NPA–NXX–XXXX in the country.

84. The CWTA is extremely concerned about the costs and practicality of creating another mechanism to maintain up-to-date and accurate CNA and LSPID information.

85. For certain services, wireless carriers do not collect CNA information for their own purpose. Any requirement to do so would impose additional costs on wireless carriers. The CWTA is concerned with the legal ramification of forcing service providers to be gate keepers of CNA information and the implication that service providers should somehow be accountable for the accuracy of said information.

Liability Issues

86. The CWTA is of the view that service providers must not be open to civil or criminal liability for any actions taken pursuant to the new law. Accordingly, the new legislation should provide appropriate safe harbour liability protection provisions for service providers. This would be consistent with the actions of other jurisdictions. The text from the New Zealand *Telecommunications (Interception Capability) Bill 2002* provides an example of liability protection clause: “Every network operator, service provider, surveillance agency and person employed or engaged by any such operator, provider or agency is protected from liability for any act done or omitted to be done in good faith under this Bill”.

87. The CWTA notes that situations have arisen (in the US) whereby the account of a mobile phone being used for illegal activities lapses into default and the service was disconnected. This has jeopardised the police surveillance. In such a situation the CWTA believes the carrier should not be held liable. Moreover, if the account is not being paid by the individual under surveillance, then the costs of maintaining the account — if required

for law enforcement purposes — should become the financial responsibility of the law enforcement agency.

88. In the situation described above and where the wireless device in question has been stolen, an additional issue arises — namely control over the phone number. Ordinarily, the stolen handset would be denied service and the rightful owner of the handset would retain his or her phone number using a new device. In such circumstances, wireless carriers must be permitted to reinstate service to the rightful account owner.

89. While some would argue that the Criminal Code provides blanket limitations on liability, it is unclear that these limitations also extend to civil matters. Moreover, it is unclear on how the blanket limitations would extend to obligations that might exist in a new law. As a result, CWTA urges the Departments to ensure that adequate safe harbour provisions are included in the new legislation.

Conclusion

90. CWTA recognizes the importance of lawful access to communications by law enforcement in Canada and appreciates the opportunity to provide these general comments on the Consultation Document. Again, CWTA notes that a number of critical questions remain unanswered regarding the proposals contained in the document. CWTA is of the view that further consultation on the details absent from the current document as well as full consultation on proposed legislation and accompanying regulations and standards, is still required.

91. Notwithstanding the above, CWTA believes that the following actions must be taken in the upcoming legislative proposals:

a. Make available sufficient federal funding for service providers:

   i. to retrofit all networks and systems to satisfy all lawful access needs of law enforcement authorities (LEAs) ;
   ii. to cover all incremental costs to provide the capability for lawful access to new networks and systems providing upgraded, significantly enhanced and new services; and
   iii. to pay service providers, as necessary, for their operational costs to provide all lawful access services that may be requested by local, regional and national law enforcement agencies.

b. The principle that law enforcement should pay service providers for assistance provided must be enshrined in the new legislation.

c. Address specific issues for licenced wireless carriers

    i. The proposals in the Consultation Document go beyond the current requirements imposed on wireless carriers for interception of circuit switched services. It is anticipated that these new obligations will significantly impact wireless carriers.
    ii. Existing Conditions of Licence for wireless carriers pertaining to the provision of lawful access should be rescinded once the new law is in force.

d. Ensure definitions are appropriate

    i. Clear definitions of the terms “Basic Intercept Capability” and “Significant Upgrade” must be established.
    ii. The definitions proposed in the Consultation Document should align with those of the *Telecommunications Act* as much as possible.
    iii. The definition of “Service Provider” should align more closely with the language of the European Convention to include “any public or private entity that provides to users of its service the ability to communicate by means of a computer system”, and “any other entity that processes or stores computer data on behalf of such communication service or users of such service.” This definition must also ensure that all competitors in the same market face the same obligations.

e. Provide for an efficient transition between regimes

    i. A transition period of at least 12 months must be provided from the enactment of the legislation to provide service providers and equipment vendors the time to understand and meet the requirements.
    ii. Forbearance decisions should be made in a fair and open process.

f. Ensure existing business processes are not unduly impacted

    i. Any requirement to provide subscriber information should be limited to that in the service provider’s possession or control.
    ii. There must not be any obligation to validate customer information.
    iii. There is no need for an additional mechanism to provide LSPID to law enforcement agencies.

g. Provide adequate liability protection for service providers

    i. Service providers must be afforded protection from civil and criminal liability for activities related to providing lawful access. As such, new legislation should provide appropriate safe harbour liability protection provisions for service providers.