THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN
The Voice of the Legal Profession
La voix de la profession juridique

May 27th, 2003

The Honourable Andy Scott, P.C., M.P.
Chair
Justice and Human Rights Committee
House of Commons
Room 622, 180 Wellington Street
Ottawa ON K1A 0A6

Dear Mr. Scott,

Re: Bill C-32, Criminal Code Amendments (setting traps)

I write on behalf of the Canadian Bar Association's National Criminal Justice Section (CBA Section) in regard to Bill C-32, Criminal Code amendments (setting traps). The CBA is a national association representing about 38,000 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice, and it is with those objectives in mind that we analyse all legislative proposals. The CBA Section includes both Crown and defence counsel from across Canada.

We appreciate this opportunity to submit our views for the Parliamentary Committee's consideration of Bill C-32. Our comments are aimed at one particular section of the Bill.

Section 4 of Bill C-32 provides a qualified exception for those in possession or control of a computer system who intercept private communications originating from, directed to, or transmitted through that system. This amendment has at least three significant effects. First, it implicitly recognizes a reasonable expectation of privacy in communications made through the use of computer networks. Second, it recognizes the need for those in possession or control of computer systems to take appropriate steps to protect those systems from malicious code or programs capable of facilitating certain Criminal Code offences. Third, it seeks to provide an exception for the interception of private communication made in the course and for the purpose of maintaining or restoring the functional ability of the system. We comment on the impact of each of these three elements in the paragraphs that follow.

500 - 865 Carling, Ottawa, **ONTARIO** Canada K1S 5S8
Tel/Tél. : (613) 237-2925 **Toll free/Sans frais :** 1-800-267-8860 **Fax/Télécop. :** (613) 237-0185
Home Page/Page d'accueil : www.cba.org **E-Mail/Courriel :** info@cba.org

The Reasonable Expectation of Privacy
The recognition of a reasonable expectation of privacy in electronic communication is a welcome and appropriate development. These forms of communication are widespread, and are used in a growing variety of circumstances. Appropriate and principled acceptance of the privacy interest inherent in many of these communications is an important step in the orderly development of the law in this area.

Computer System Protection
The need to protect computer networks from malicious or harmful programs or code is well understood. Section 4 provides a narrow exception that enables the interception of what would otherwise be private communication for the specified purpose of defending networks against specified criminal acts. This aspect of section 4 provides appropriate clarification on the use of practices and devices designed and intended to protect the computer system.

System Management and Quality of Service
The third aspect of section 4, however, is a cause of significant concern. This concern arises both from the expansive language proposed, and the particular nature of the material likely to be intercepted.

Clearly, those in possession or control of computer systems need to manage, maintain and restore function to those networks. This need is analogous to that of telecommunication service providers who must be able to access communications in specified circumstances. Section 184 (2)(c) of the Code provides exceptions clearly describing those circumstances in the following terms:

(2) Subsection (1) does not apply to

(c) a person engaged in providing a telephone, telegraph or other communication service to the public who intercepts a private communication,

(i) if the interception is necessary for the purpose of providing the service,

(ii) in the course of service observing or random monitoring necessary for the purpose of mechanical or service quality control checks, or

(iii) if the interception is necessary to protect the person's rights or property directly related to providing the service; or

This contrasts with the language of the proposed section 4, which describes this aspect of the exception merely as “for the purpose of managing the computer system for quality of service”. The general nature of this provision gives rise to several concerns.

First, it gives no meaningful or practical guidance to those in possession or control of computer networks, the legal community, or the courts regarding the scope of actions that may be justified under this exception.

Second, it fails to distinguish between the technical or functional aspects of the communication, and the content of the communication itself. The section should clearly indicate that the only rationale for targeting the content of a communication is to protect the network from listed Criminal Code offences. A separate exception relating to system management could be drafted to focus on the technical aspects or functional impact of the communication on the system, for example, issues such as file or attachment size, frequency or volume of communication, or any other patterns or issues relating to the management of communication traffic or volume on the computer system. The section should clearly describe that in relation to the issue of network management, quality of service relates only to the functional ability of the network.

Failure to circumscribe the terms "managing the computer system" and "quality of service", clearly and narrowly, fundamentally erodes the very expectation of privacy on which the legislative proposal is obviously based. The breadth of this exception, as presently worded, seriousy undermines the recognition of reasonable expectations of privacy.

Past experience with the interpretation of section 184(2)(c)(iii) illustrates that such general language leads to expansive interpretations that significantly enlarge the scope of the exceptions in question.

Furthermore, as drafted, the exception fails to account for the unique nature of the written communication likely to be intercepted on computer networks. Unlike the interceptions that may occur within the scope of existing exceptions in the context of oral telecommunications, where fragments or portions of verbal communications may be intercepted, the written nature of communications used in computer networks dramatically increases the likelihood of intercepting a significantly greater portion of the communication. As a result, very brief interceptions of written communications may well secure much more information than their audio equivalent. This magnifies the impact of even brief or incidental interceptions. This fact alone requires greater care and circumspection in drafting this aspect of the exception.

In light of the above, we are strongly of the view that the exception for "managing the quality of service" should be clearly and carefully defined. Language that clearly confines the exception to the functional capacity of the network should be used.

For example, the distinct elements of the exception could be separated as follows:

(2) Subsection (1) does not apply to

(e) a person, or any person acting on their behalf, in possession or control of a computer system, as defined in subsection 342.1(2), who intercept a private communication originating from, directed to or transmitting through that computer system,

(i) for the purpose of protecting the computer system against any act that would be an offence under subsection 342.1(1) or 430(1.1); or,

(ii) in the course of managing the volume and flow of communications and other data within and across the computer system for the purpose of maintaining the capacity and functional operation of the computer system

This wording is provided as an example only, and is intended to reflect the descriptive nature of the language required to appropriately delineate this exception. Technological realities may well dictate the use of other specific language to describe accurately the functions and processes in question.

Conclusion

While we do not disagree with the general objectives of proposed section 4, we have serious concerns about the very expansive and general language suggested to achieve those objectives. These concerns are especially strong with respect to the phrase "managing the computer system for quality of service". This general language may well frustrate the other objectives of this section.

Thank you for considering the views of the CBA Section.

Yours truly,

Kate Ker
Chair
National Criminal Justice Section