

BILL C-17: THE PUBLIC SAFETY ACT, 2002

Prepared by:

David Goetz, David Johansen, Margaret Young, Law and Government Division

Michel Rossignol, Political and Social Affairs Division

Jean-Luc Bourdages, François Côté, Science and Technology Division

15 November 2002

Revised 8 May 2003

E. Computer Systems and Networks and Commissioner of the Communications Security Establishment

Clause 78 creates a new Part V.2 of the Act, dealing with the interceptions of communications involving the Department of National Defence (DND) or Canadian Forces computer systems. This new provision ensures that DND and the Canadian Forces have the authority to protect their computer systems networks and the information they contain from attack or manipulation. The vulnerability of computer systems to interference and outright attacks has been a growing concern in recent years, especially within military forces, which are increasingly dependent on information technology for success on the battlefield and for carrying out other operations. Although various measures have been taken to protect the computer systems used by the department and the Forces from intrusions from outside sources, protection is also needed against actions from within the department or Forces that can accidentally or deliberately damage the systems. For example, someone from outside the department or the Forces could send an e-mail which could subsequently damage military computer systems or networks, or someone within the department or the Forces could sabotage systems or networks or use them for purposes which contravene the Code of Military Discipline or the *Criminal Code*.

New section 273.8 allows the Minister of National Defence to authorize in writing public servants in the department or persons acting on behalf of the department or the Forces who operate, maintain or protect computers and networks to intercept private communications. Sections 273.7(1) and (2) in Bill C-42 described the private communications as “originating from, directed to or transiting through any” computer system or network. Sections 273.8(1) and (2) in Bill C-55 and now Bill C-17 go into greater detail, since they state that these communications are “in relation to an activity or class of activities specified in the authorization, if such communications originate from, are directed to or transit through” any computer system or network.

The interception can be carried out only in order to identify, isolate or prevent (a) the unauthorized use of, interference with, or damage to departmental and military computer systems or networks, and (b) damage to the data they contain. Compared to Bill C-55, Bill C-17 is more specific. Bill C-55 referred to the

unauthorized use of, interference with, or damage to systems, networks, or the data they contain. In Bill C-17, the words “any damage to” were added in front of the words “the data that they contain” at the end of sections 273.8(1), 273.8(2), 273.8(3)(a), 273.8(3)(d), and 273.8(9)(a). The new wording and the comma added after the word “networks” imply that intercepts can be carried out in order to identify, isolate or prevent damage to data as well as the unauthorized use of, interference with, or damage to system or networks. The Minister may authorize in writing interceptions by public servants employed in the department or any person acting on behalf of the department or the Canadian Forces. The Minister may also authorize in writing the Chief of the Defence staff to direct military personnel to carry out interceptions. In either case, the Minister must be satisfied that certain conditions are met. These are that:

- the interception is necessary to identify, isolate or prevent (a) “any harmful” unauthorized use of, “any” interference with, or “any” damage to the systems or networks, or (b) damage to the data, and that measures are in place to ensure that only information that is essential for these purposes will be used or retained (the words within quotation marks are in sections 273.8(1), (2) and (3) of Bill C-17, as well as in Bill C-55, but were not in the corresponding sections in Bill C-42);
- the information cannot be reasonably obtained by other means; and
- measures are in place to protect Canadians’ privacy in the use or retention of the information.

According to section 273.8(4), authorizations may contain conditions to protect the privacy of Canadians. While Bill C-42 mentioned information “derived from” private communications, Bill C-17, like Bill C-55, says “contained in.” Authorizations or renewals are for periods not exceeding one year. Part VI of the *Criminal Code*, which otherwise prohibits the interception of private communications occurring within Canada, does not apply. In addition, according to section 273.8(9), government officials are not civilly liable for improper disclosure or use of intercepted information under section 18 of the *Crown Liability and Proceedings Act*.

During the First Session of the Thirty-seventh Parliament, some amendments to the *National Defence Act* were also made in Bill C-36, the *Anti-terrorism Act*. Thus, clause 78 also adds new section 273.9 to the Act. The new section indicates the duties of the Commissioner of the Communications Security Establishment (CSE) with regard to the interception of communications originating from, directed to, or transiting through departmental or military computer systems and networks. The Commissioner of the CSE has jurisdiction to: review the activities of the department and the Forces to ensure compliance with the law, and to report annually to the Minister on the review; undertake an investigation in response to a complaint; and inform the Minister of National

Defence and, if appropriate, the Attorney General if any activity of the department or the Forces does not appear to be in compliance with the law.