

OUTSIDE PERSPECTIVES

Canada's Lawful Access Proposals - Increased Obligations On Service Providers

BRUCE McWILLIAM

The Canadian Department of Justice has released a Consultation Document entitled "Lawful Access", containing proposals to enhance the ability of law enforcement and national security agencies to intercept electronic communications and search for and seize information. The document also calls for comments on related topics, including the creation of a new virus dissemination offence, clarification of the status of e-mail messages for interception purposes, and the establishment of a nation-wide database of subscriber information.

The Changing World of Crime

The Consultation Document correctly points out that authorities face increasing challenges in conducting investigations in the face of ever-changing technology. In the past, a properly authorized wiretap could be used for interception of telephone conversations. However, legislation created for POTS (plain old telephone service) may need to be updated to deal with new technologies. Also included in the justifications for the proposals is Canada's signature on the November 23, 2001 Council of Europe *Convention on Cyber-Crime*.

Of particular interest to Internet

and telecommunications service providers are the increased obligations that may be imposed on them by the proposed new rules. Depending on the details, these may have significant cost, personnel and operational impact.

The Proposals – Interception Orders

The first proposal would require service providers to have the technical capability to allow interception of communications (both content and traffic data) by lawfully authorized agencies. The extent of the obligations is not discussed, including whether only "raw data" or processed data would be required. However, regulations would prescribe technical and other standards and requirements, security requirements for intercepted information, capacity requirements for the number of simultaneous interceptions, and the competence, reliability and deployment of employees. These requirements could require service providers to make significant investments in new equipment and software, and employment and training of personnel. The proposals suggest that service providers would not bear the cost of changes to existing systems or networks, but would pay for compliance in respect of new or upgraded technologies, services and networks.

In contrast, the *Convention on Cyber-Crime* requires a service provider to collect and record data, and co-operate and assist, only "within its existing technical capability". This is amplified in the *Explanatory Report* accompanying the Convention, which states that "[t]he article does not obligate service providers to ensure that they have the technical capability to undertake collections, recordings, co-operation or assistance. It does not require them to acquire or develop new equipment, hire expert support or engage in costly re-configuration of their systems."

Data Preservation Orders

Another proposal is for a new, data preservation order. This would be an expedited order requiring service providers to store and save existing data specific to a transaction or client. The order would remain in effect only until authorities obtain a judicial warrant to seize the data, or a production order to deliver the data. Preservation orders differ from retention orders, which would require retention of data generally for all customers.

If the intention is merely to prevent premature deletion of data, the impact would be less onerous. However, if service providers must retain data longer than their usual practice, they would likely incur increased costs, in terms of equipment, person-

DOING BUSINESS IN CANADA

nel and processes. Also, retaining the data of one customer for a period of time might as a practical matter involve either retaining all raw data for all customers for that period, or doing extra processing to assemble the subject's data in intelligible form.

The proposal also suggests that in exigent circumstances, authorities should be able to require a service provider to preserve data without a judicial order for a specified period such as four days, if the conditions for obtaining a judicial order exist but it would be impracticable to obtain one. Similar provisions to this are already included in the *Criminal Code* (Canada) in respect of search warrants and wiretaps.

Production Orders

The proposals also include suggestions for production orders for Internet traffic data and similar information. For these there would be lowered safeguards in terms of availability and protection of privacy and other rights. The Consultation Document suggests that this is justified on the basis that there is a lower expectation of privacy for such information. However, this depends, among other things, on how "traffic data" is defined – does it mean an Internet Protocol (IP) address (such as *198.104.177.91*), the main web site Uniform Resource Locator (such as *www.mcmillanbinch.com*), or the URL resulting from a user's request to a search engine (such as *http://.../search?q=lawful+access&i*

e=UTF-8&oe=UTF-8&hl=en&meta=, produced when searching "lawful access"), which discloses content in addition to traffic information?

Other Requirements

In other cases, the document raises the possibility of a service provider being required to collect and provide information that it would not otherwise collect or retain for its own purposes (such as certain name, address and service provider information), and being subject to anticipatory production orders (permitting authorities to monitor transactions for a specified period of time in circumstances that would not allow a production order).

The Responses

The proposals have been the subject of comments from service providers, privacy groups and others. Concerns have been raised about costs incurred by service providers and their users, the need to maintain privacy and other rights, including protection against self-incrimination, and appropriate requirements for judicial authorization and limitations on the power granted to authorities.

In addition, it will be necessary to consider the appropriateness of requiring service providers to collect and provide information for government purposes beyond what they need for their own businesses, as well as the rules that apply to the information and the service provider. These issues include whether priva-

cy legislation continues to apply to the information, and to what extent the *Canadian Charter of Rights and Freedoms* applies in respect of the actions of the service provider.

One response to the Consultation Document has been that more details are required in order to understand the implications of the proposals. When and if further details are provided, more meaningful analysis will be possible.

Bruce McWilliam is a partner in the KNOWlaw™ Group of the Toronto law firm McMillan Binch LLP. He was called to the Ontario bar in 1985 and practices business law with an emphasis on technology and telecommunications matters.

MCMILLAN BINCH LLP
