



The rate at which new wireless technologies and services are being introduced to the public makes it challenging for law enforcement and national security agencies to maintain their technical ability to lawfully intercept communications. Furthermore, the global nature of such technologies can pose significant jurisdictional problems in criminal and terrorist investigations.

In addition to wireline and wireless communications, investigative bodies are facing challenges relating to the Internet as a result of the technology used for Internet communications, the need for sophisticated equipment to lawfully intercept Internet communications, and the lack of provisions requiring Internet service providers to implement procedures for lawful intercept capabilities.

Lawful access is essential for law enforcement and national security agencies to conduct investigations. In regards to telecommunications in Canada, it involves the interception of communications as well as search and seizure of information under the Criminal Code, the Canadian Security Intelligence Service Act, and other legislation such as the Competition Act.

These acts give law enforcement agencies the power to intercept communications and search and seize information in a manner consistent with Charter rights.

They utilize lawful access in the prevention, investigation, and prosecution of serious offences and the investigation of threats to the security of Canada. According to the federal government, updating lawful access legislation is necessary to such investigative bodies to assist them in efforts to combat crimes such as child pornography, drug trafficking, Internet and telemarketing fraud, money laundering, smuggling, price fixing, and terrorism.

Currently, Canada does not have a mechanism

to describe what providers must do to allow access to their facilities, security requirements relating to how intercepted information is handled, and the manner in which regulations are to be developed.

Several amendments to the Criminal Code have been proposed to deal with interception and search and seizure provisions, and to permit Canada to ratify Europe's Convention on Cyber-Crime. They relate to production orders, orders to obtain subscriber and/or service provider information, assistance orders, data-preservation orders, virus dissemination, and interception of e-mail.

In addition, the Competition Act should be amended with respect to access to hidden records along with other orders such as general warrants and assistance orders in order to enhance the efficacy of evidence gathering tools.

A preservation order is a procedural mechanism in the Convention on Cyber-Crime that does not exist in Canadian law. In essence, it acts as an expedited judicial order requiring a service provider to store and save existing data specific to a client or transaction. A preservation order is temporary and only remains in effect for as long as it takes law enforcement agencies to obtain a production order requiring delivery of the data or a judicial warrant to seize the data. Their purpose is to ensure information crucial to an investigation is not deleted prior to law enforcement officials being able to obtain a production order or search warrant.

They are different from a more general requirement that service providers collect and retain a variety of data relating to all of their subscribers.

There are also various issues relating to the interception of e-mail. Part VI of the Criminal Code creates an offence for willfully

obtaining information on the subjects of their investigations in order to determine where to target an interception. Determining the local service provider identification (LSPID) information is the first step in identifying a subscriber. However, the only way this information can be obtained is through a time-consuming and costly process of directly contacting each local carrier.

The Canadian Radio-television and Telecommunications Commission recently approved the conditions under which Bell Canada could release LSPID information without a court order — for emergency, national security, and law enforcement purposes.

A related issue is how investigators can obtain access to customer names and addresses, bearing in mind that some service providers do not even collect or store them.

The Canadian Association of Chiefs of Police has recommended ways to improve lawful access to this information, including the establishment of a national database. Such implementation would presuppose service providers are compelled to provide accurate and current information, which raises the issue of whether or not a provider should be compelled by law to collect names and addresses if it does not already collect them for its own purposes, who should bear the costs of collecting, retaining, and accessing the information, and, if a database were to be established, who should operate it.

The government will meet with interested parties this fall to discuss lawful access issues. A copy of the discussion paper can be obtained at www.canada.justice.gc.ca/en/cons/la_allb.html#6.

LT

Alan Gahtan (agahtan@mann
gahtan.com) is a partner with Mann
& Gahtan LLP and with Brown,
Raysman Millstein Felder & Stein