Bill C-22 embraced by law enforcement officials as way to help curb online crime

Written By Mark Pavilons

Law enforcement officials across the province are welcoming changes contained in Bill C-22 (Part 2), that focus on electronic service providers (ESPs).

The Bill, Securing Access to Information (Bill C-22 ? Part 2), aims to curb criminals who exploit the use of the ?digital ecosystem? and carry out online crimes of various descriptions.

Public Safety Canada notes law enforcement agencies and CSIS have worked for decades with ?outdated laws that have not kept pace with our new technological and digital reality. As a result, investigations are missing critical information needed to generate leads or help identify and prosecute individuals or groups involved in serious criminal activities or national security threats. In some cases, investigations are abandoned due to these challenges.?

Part 2 of the Bill C-22 does not create new authorities for law enforcement agencies and CSIS to intercept communications or obtain information. It focuses solely on ensuring that electronic service providers (ESPs) are able to comply with existing legal orders, which are found in the Criminal Code, and the Canadian Security Intelligence Service Act.

Currently, Canada relies on a 1995 condition of license that only covers voice telephony despite vast technological changes, including the internet, satellite and messaging platforms. Law enforcement agencies and CSIS can obtain authorization, though a warrant or production order, to intercept communications or obtain information; however, there is no corresponding requirement for an ESP to actually establish and maintain a system capable of providing the communication/information in question. Furthermore, outside of voice telephony services, the support of ESPs to fulfill lawful access requests is entirely voluntary.

The Bill would require select ESPs, to develop and maintain the capabilities necessary to enable law enforcement and CSIS to effectively obtain communications and information they are legally authorized to have for their criminal and intelligence investigations, while respecting rights and freedoms.

Instead of requiring whole sectors, including small enterprises, to have the same capabilities in place, the proposed framework adopts a more targeted approach for technical capability development. Under the proposed Bill, there are two ways by which an ESP could be mandated to develop and maintain lawful access capabilities: ESPs designated as ?core providers' and through Ministerial Orders.

The Minister of Public Safety could issue a Ministerial Order (MO), subject to approval by the Intelligence Commissioner, to electronic service providers (ESP) compelling the development of specific capabilities. MOs would be based on operational needs, as threats evolve and new technologies develop, and could be issued to both core and non-core providers. In deciding whether to issue an MO, the Minister must consider the same factors as the Governor in Council when making regulations for core-providers. MOs would be reviewable by the courts.

MOs are a powerful tool that allow the Minister of Public Safety to request a broad range of technical capabilities in a confidential way to avoid tipping off threat actors. The Intelligence Commissioner's role in MO approvals strengthens the framework by providing an external oversight mechanism. The addition of an annual report and parliamentary review, three years after the Act comes into force, further increases transparency.

Currently, law enforcement and CSIS may have the legal authority to obtain information from ESPs, but there are no laws that require ESPs to maintain a system that can effectively respond to requests. This means that despite having the requested communications and information in their systems, an ESP may be unable to provide it. This lack of technical capability has caused investigations to stall or not begin at all. The issue can be as simple as an ESP not having the secure infrastructure to transfer

information to these agencies in a useable format. In other cases, they may not be able to retrieve the information within a certain timeline, or to ensure its accuracy.

Compliance enforcement under the current framework is extremely limited.

To promote compliance, SAAIA would create monetary penalties for contravening obligations under the Act. SAAIA sets out parameters for the issuance of administrative penalties, including in what amount and how an ESP can request a review from the Minister.

In addition to administrative monetary penalties, SAAIA also contains offences for contravening provisions.

Penalties are required to make sure that a regulatory regime can be properly enforced.

Proposals under Bill C-22 provide additional oversight and transparency.