THE PRICE OF PEEKING

Bill C-30 sends the signal Canada is open for 'Big Brother Inc.' business

By Michael Geist

Last year, Privacy International—one of the world's leading privacy organizations—released the results of a multi-year investigation into the shadowy world of the commercial surveillance industry. Dubbed "Big Brother Inc.," the investigation placed the spotlight on more than 100 companies that specialize in covert surveillance technologies, which are typically sold to governments and law enforcement agencies.

Governments in Asia and the Middle East have provided a ready market for technologies that can monitor Internet activities and create a chilling effect on freedom of expression. But Canada is not innocent in this regard. New online surveillance legislation, Bill C-30, features provisions that appear to open the door to using such tools.

The Privacy International investigation revealed that surveillance companies commonly promote virtually unlimited monitoring capabilities to governments and police agencies. For example, Italian-based Innova offers "solutions for the interception of any kind of protocols and IP-based communication, such as web browsing, email and web-mails, social networks, peer to peer communication, chat and videochat." Endace Accelerated, a New Zealand-based company, promotes the "power to see all for Government," and the U.K.-based Gamma Group offers "turnkey lawful interception projects" that include SMS interception, speech identifying tools and data retention.

In all, the investigation reveals how online surveillance has become a massive global industry—one that makes it easy for law enforcement agencies to implement surveillance capabilities, and send a disturbing message that online expression can be tracked and monitored.

Some Canadian companies, including B.C.-based Vineyard Networks, that specialize in deep packet inspection of Internet traffic for lawful interception purposes were included in the report. Deep packet inspection allows Internet service providers (ISPs) and other network providers to look at parts of messages and transmissions over a network; it's often used to keep networks secure, but has also been used to infer the habits of consumers. Yet more important than the existing Canadian surveillance industry is the potential market in Canada for surveillance technologies.

Most of the attention on proposed Canadian Internet surveillance legislation has focused on the mandatory disclosure of Internet and telephone subscriber information without court oversight. But just as troubling is the plan to create a massive new surveillance infrastructure, which has enormous free speech and privacy implications.

Bill C-30 requires ISPs to acquire the ability to engage in multiple simultaneous interceptions, and gives law enforcement agencies and officials the power to audit their surveillance capabilities. Should it take effect, the Bill would create a new regulatory environment for ISPs, requiring them to submit a report describing their equipment and surveillance infrastructure within months of the law taking effect. Moreover, they would actively work with law enforcement agencies to test their facilities for interception purposes, and even provide the name of employees involved in interceptions to allow for possible RCMP background checks.

In addition to the surveillance requirements, the Bill would also give the government the power to install its own equipment directly onto private Internet provider networks. Section 14(4) states: "The Minister may provide the telecommunications service provider with any equipment or other thing that the Minister considers the service provider needs to comply with an order made under this section."

This amounts to giving government the power to decide what specific surveillance equipment must be installed on private ISP and telecom networks.

With ongoing doubts about the ability of Canadian ISPs to pay the multimillion-dollar costs associated with new surveillance equipment (and some speculation the government is prepared to provide tens of millions of dollars in assistance), the government may ultimately shift toward a model in which it buys the surveillance equipment and uses Section 14(4) to require the Internet providers to install it. If that is what the government has in mind, Bill C-30 will soon look like a giant Canadian "open for business" sign to Big Brother Inc., placing freedom of expression at risk.

Michael Geist holds the Canada Research Chair in Internet and E-commerce Law at the University of Ottawa, Faculty of Law. He can reached at mgeist@uottawa.ca or online at michaelgeist.ca.