MINISTRY OF PUBLIC SAFETY AND SOLICITOR GENERAL
POLICING AND COMMUNITY SAFETY BRANCH
POLICE SERVICES DIVISION
BRIEFING NOTE

PREPARED FOR: Minister Kash Heed, Solicitor General, for February 25th, 2010 meeting with Minister Toews

ISSUE: Lawful Access

S13

BACKGROUND:

- The provisions of the *Criminal Code* that deal with wiretap were drafted to cover voice communications before the era of the Internet and wireless data communication. The definition of a private communication in the *Code* is phrased in a manner that is ambiguous as to whether it covers electronic text communications. Given the ambiguity as to where new communications technologies fit within the statutory scheme, clarification is desirable.

- Since the original philosophy behind the wiretap provisions (Part VI of the *Criminal Code*) was that voice communications were afforded special protection, requiring interception to be the last practical resort, the definition of private communication should be clarified to exclude all text based communications such as emails, chat, SMS (text messages) and PIN. This would permit police the ability to seize the text communications using a warrant or intercept them using a general warrant and would remove ambiguity as to what constitutes a private communication. This is consistent with the original philosophy behind Part VI.

- Currently some cell/wireless network companies are not retaining text message data. This business decision seriously impedes police investigations where text message communication between suspects is critical evidence of criminality.

Organized Crime and New Technologies

- In the past, cybercrimes such as hacking were largely perpetrated by individuals to show that they had a level of expertise and could get past sophisticated security systems. However, the profile and the motives behind on-line crime have changed in the past decade, as have the crimes themselves. The blended sophisticated types of on-line crime are aimed at large financial gains and are often the work of organized crime groups. Organized crime has been linked to the use of botnets; credit card fraud; and ATM overlays, as well as other computer crimes. Internationally, experts are witnessing linkages between organized crime groups and the commission of high-tech crimes. With the increasing popularity of the Internet and e-commerce within Canada, organized crime groups have recognized a lucrative opportunity in which they can make significant amounts of money with low risk of detection.

Lawful Access

- 'Lawful access' consists of the lawful interception of communications and the search and seizure of information. Lawful access supports the full range of investigative and intelligence gathering activities carried out by law enforcement agencies at the federal, provincial and municipal levels, and by the Canadian Security Intelligence Service (CSIS).[1]

- Lawful access is an essential tool at both the domestic and international level in the prevention, investigation and prosecution of serious offences, such as organized crime activities, murder and kidnapping.

- The CCSO Working Group on Cyber-crime (CWG), which is co-chaired by British Columbia, has focused on this issue since the group's inception in 2001. It has been long recognized that there was need to update the search and seizure and intercept provisions in the *Criminal Code*. The challenge for the federal government has been in developing legislation that would modernize investigations techniques, but maintain a balance with privacy and human rights and freedoms.

Lawful Access Proposals to Amend the Criminal Code

-

S13, S16

[1] Status Report from Justice Canada and Public Safety and Emergency Preparedness Canada, November 2005

S13, S16

Bills 46 and 47

- C-46 provides police with powers to 'freeze' evidence held by the ISP, through preservation demands and preservation orders. This allows law enforcement the time to apply for production orders, which would compel the ISP to give police existing transmission data showing the features of when and where messages were sent, as well as other characteristics such as the length of messages.

- It will also expand warrants allowing police to seize current and future transmission information whether the communication originates from 'land line' telephones, wireless devices or computers.

- C-46 will expand the ability of police to obtain information that will assist them in determining the location of a transaction, a person or a thing (such as a cell phone or car). A tracking production order will compel ISPs to provide police with existing information, and amendments to tracking warrants will allow police to remotely activate a tracking device to obtain this information.

- C-47 requires ISPs and telecoms to provide police with customer name and address (CNA) as well as other identifiers, such as the person's IP address, if required for an investigation. It will also require telecommunication service providers to ensure that their equipment and technology is 'intercept capable' and does not prevent the police from obtaining information pursuant to a court order. Initially this requirement applies to larger companies, with a three-year phase-in period allowing smaller companies time to acquire the necessary technology to comply.

- While the bulk of this legislative package is relevant to lawful access, C-46 also amends specific offences to reflect the use of new technologies. These offences include hate propaganda and its communication over the Internet, false information, indecent communications, harassing communications, devices used to obtain telecommunication services without payment and devices used to obtain the unauthorized use of computer systems or to commit mischief. It also creates a new offence of agreeing or arranging with another person by a means of telecommunication to commit a sexual offence against a child.

- Both bills died on the order paper when parliament was prorogued.

Prepared by: Mark Tatchell
Telephone No.: 250 387 2036
Date: February 23, 2010
CLIFF: 383869
Approved by: Kevin Begg
Assistant Deputy Minister
Policing and Community Safety Branch
February 24, 2010